kaspersky

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready

Содержание

Часто задаваемые вопросы

ОБЩЕЕ

РАЗВЕРТЫВАНИЕ

ОБНОВЛЕНИЕ

БЕЗОПАСНОСТЬ

ИНТЕРНЕТ

ПРОГРАММЫ

УСТРОЙСТВА

ШИФРОВАНИЕ

ПОДДЕРЖКА

[Как восстановить файл, который Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready ошибочно удалил?]

[Как защитить Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready от удаления пользователем?]

Что нового

В Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.4.0 появились следующие возможности и улучшения:

1. Обновлен дизайн значка программы в области уведомлений. Вместо значка теперь используется значок . Если от пользователя требуется выполнить действие (например, перезагрузить компьютер после обновления программы), значок изменится на . Если работа компонентов защиты программы выключена или нарушена, значок изменится на или . Если навести курсор на значок, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready покажет описание проблемы в защите компьютера.

2. Программа Kaspersky Endpoint Agent, входящая в комплект поставки, обновлена до версии 3.9. Kaspersky Endpoint Agent 3.9 поддерживает интеграцию с новыми решениями "Лаборатории Касперского".
   Подробнее об интеграции с решениями "Лаборатории Касперского" см. в справке Kaspersky Endpoint Agent.

3. Добавлен статус Не поддерживается лицензией для компонентов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Вы можете просмотреть статус компонентов по кнопке Компоненты защиты в главном окне программы.

4. В отчеты добавлены новые события о работе компонента Защита от эксплойтов.

5. Драйверы для работы технологии Шифрование диска Kaspersky автоматически добавляются в среду восстановления Windows (англ. WinRE – Windows Recovery Environment) при запуске шифрования диска. В предыдущей версии программа добавляла драйверы при установке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Добавление драйверов в WinRE позволяет повысить стабильность работы программы при восстановлении операционной системы на компьютерах, защищенных технологией Шифрование диска Kaspersky.

Компонент Endpoint Sensor исключен из программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Вы можете продолжать настраивать параметры Endpoint Sensor с помощью политики, если на компьютере установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready версий 11.0.0 – 11.3.0.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (далее также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready) обеспечивает комплексную защиту компьютера от различного вида угроз, сетевых и мошеннических атак.

Каждый тип угроз обрабатывается отдельным компонентом. Можно включать и выключать компоненты независимо друг от друга, а также настраивать параметры их работы.

К компонентам контроля относятся следующие компоненты программы:

- Контроль программ. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.

- Контроль устройств. Компонент позволяет установить гибкие ограничения доступа к устройствам, являющимся источниками информации (например, жесткие диски, съемные диски, CD/DVD-диски),

инструментами передачи информации (например, модемы), инструментами преобразования информации (например, принтеры) или интерфейсами, с помощью которых устройства подключаются к компьютеру (например, USB, Bluetooth).

- Веб-Контроль. Компонент позволяет установить гибкие ограничения доступа к веб-ресурсам для разных групп пользователей.

- Адаптивный контроль аномалий. Компонент отслеживает и регулирует потенциально опасные действия, нехарактерные для защищаемого компьютера.

К компонентам защиты относятся следующие компоненты программы:

- Анализ поведения. Компонент получает данные о действиях программ на вашем компьютере и предоставляет эту информацию другим компонентам для более эффективной защиты.

- Защита от эксплойтов. Компонент отслеживает исполняемые файлы, запускаемые уязвимыми программами. Если попытка запустить исполняемый файл из уязвимой программы не была инициирована пользователем, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует запуск этого файла.

- Предотвращение вторжений. Компонент регистрирует действия, совершаемые программами в операционной системе, и регулирует действия программ исходя из того, к какой группе компонент относит эту программу. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к персональным данным пользователя и ресурсам операционной системы. К таким данным относятся файлы пользователя в папке "Документы", файлы cookie, файлы с историей активности пользователя, а также файлы, папки и ключи реестра, содержащие параметры работы и важные данные наиболее часто используемых программ.

- Откат вредоносных действий. Компонент позволяет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отменить действия, произведенные вредоносными программами в операционной системе.

- Защита от файловых угроз. Компонент позволяет избежать заражения файловой системы компьютера. Компонент начинает работать сразу после запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на компьютере и на всех присоединенных запоминающих устройствах. Компонент перехватывает каждое обращение к файлу и проверяет этот файл на присутствие вирусов и других программ, представляющих угрозу.

- Защита от веб-угроз. Компонент проверяет трафик, поступающий на компьютер пользователя по протоколам HTTP и FTP, а также устанавливает принадлежность веб-адресов к вредоносным или фишинговым.

- Защита от почтовых угроз. Компонент проверяет входящие и исходящие сообщения электронной почты на наличие вирусов и других программ, представляющих угрозу.

- Защита от сетевых угроз. Компонент отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует сетевую активность атакующего компьютера.

- Сетевой экран. Компонент обеспечивает защиту данных, хранящихся на компьютере пользователя, блокируя большинство возможных для операционной системы угроз в то время, когда компьютер подключен к интернету или к локальной сети.

- Защита от атак BadUSB. Компонент позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

- Поставщик AMSI-защиты. Компонент проверяет объекты по запросу от сторонних приложений и сообщает результат проверки тому приложению, от которого был получен запрос.

В дополнение к постоянной защите, реализуемой компонентами программы, рекомендуется периодически выполнять проверку компьютера на присутствие вирусов и других программ, представляющих угрозу. Это нужно делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами, например, из-за установленного низкого уровня защиты.

Чтобы поддерживать защиту компьютера в актуальном состоянии, требуется обновление баз и модулей программы, используемых в работе программы. По умолчанию программа обновляется автоматически, но при необходимости вы можете вручную обновить базы и модули программы.

В программе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предусмотрены следующие задачи:

- Проверка целостности. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет модули программы, находящиеся в папке установки программы, на наличие повреждений или изменений. Если модуль программы имеет некорректную цифровую подпись, то такой модуль считается поврежденным.

- Полная проверка. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет проверку операционной системы, включая память ядра, загружаемые при запуске операционной системы объекты, загрузочные секторы, резервное хранилище операционной системы, а также все жесткие и съемные диски.

- Выборочная проверка. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет объекты, выбранные пользователем.
-

Проверка важных областей. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет память ядра, загружаемые при запуске операционной системы объекты и загрузочные секторы.

- Обновление. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready загружает обновленные базы и модули программы. Это обеспечивает актуальность защиты компьютера от вирусов и других программ, представляющих угрозу.

- Откат последнего обновления. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отменяет последнее обновление баз и модулей. Это позволяет вернуться к использованию предыдущих баз и модулей программы при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует безопасную программу.

Служебные функции программы

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready включает ряд служебных функций. Служебные функции предусмотрены для поддержки программы в актуальном состоянии, для расширения возможностей использования программы, для оказания помощи в работе.

- Отчеты. В процессе работы программы для каждого компонента формируется отчет. Также в отчетах вы можете отслеживать результаты выполнения задач. Отчеты содержат списки событий,

произошедших во время работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, и всех выполненных программой операций. В случае возникновения проблем отчеты можно отправлять в "Лабораторию Касперского", чтобы специалисты Службы технической поддержки могли подробнее изучить ситуацию.

- Хранилище данных. Если в ходе проверки компьютера на вирусы и другие программы, представляющие угрозу, программа обнаруживает зараженные файлы, она блокирует эти файлы. Копии вылеченных и удаленных файлов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет в резервном хранилище. Файлы, которые не были обработаны по каким-либо причинам, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready помещает в список активных угроз. Вы можете проверять файлы, восстанавливать файлы в папку их исходного размещения, а также очищать хранилище данных.

- Служба уведомлений. Служба уведомлений позволяет пользователю отслеживать события, влияющие на состояние защиты компьютера и работу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Уведомления могут доставляться на экран или по электронной почте.

- Kaspersky Security Network. Участие пользователя в Kaspersky Security Network позволяет повысить эффективность защиты компьютера за счет оперативного использования информации о репутации файлов, веб-ресурсов и программного обеспечения, полученной от пользователей во всем мире.

- Лицензия. Приобретение лицензии обеспечивает полнофункциональную работу программы, доступ к обновлению баз и модулей программы, а также консультации по телефону и электронной почте по вопросам, связанным с установкой, настройкой и использованием программы.

- Поддержка. Все зарегистрированные пользователи Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready могут обращаться за помощью к специалистам Службы технической поддержки. Вы можете отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount или позвонить в Службу технической поддержки по телефону.

Если во время работы программы возникают ошибки или зависания, программа может быть автоматически перезапущена.

Если в работе программы возникают повторяющиеся ошибки, которые приводят к прекращению работы, программа выполняет следующие действия:

1. Выключает функции контроля и защиты (функция шифрования продолжает работать).
2. Уведомляет пользователя о выключении функций.
3. После обновления антивирусных баз или применения обновлений модулей программы пытается восстановить работоспособность.

Комплект поставки

Комплект поставки содержит следующие дистрибутивы:

- Strong encryption (AES256)

  Дистрибутив содержит криптографические средства, реализующие криптографический алгоритм AES (Advanced Encryption Standard) с эффективной длиной ключа 256 бит.

- Lite encryption (AES56)

  Дистрибутив содержит криптографические средства, реализующие криптографический алгоритм AES с эффективной длиной ключа 56 бит.

Каждый дистрибутив содержит следующие файлы:

`kes_win.msi`	Пакет установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.
`setup_kes.exe`	Файлы, необходимые для установки программы всеми доступными способами.
`kes_win.kud`	Файл для создания инсталляционного пакета Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.
`klcfginst.msi`	Пакет установки плагина управления Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Kaspersky Security Center.
`bases.cab`	Файлы пакетов обновлений, которые используются при установке программы.
`cleaner.cab`	Файлы для удаления несовместимого программного обеспечения.
`incompatible.txt`	Файл со списком несовместимого программного обеспечения.
`ksn_<ID языка>.txt`	Файл, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Security Network.
`license.txt`	Файл, с помощью которого вы можете ознакомиться с Лицензионным соглашением и Политикой конфиденциальности.
`installer.ini`	Файл, содержащий внутренние параметры дистрибутива.
`endpointagent.msi`	Пакет установки программы Kaspersky Endpoint Agent, необходимой для интеграции с другими решениями "Лаборатории Касперского" (например, Kaspersky Sandbox).

Не рекомендуется изменять значения этих параметров. Если вы хотите изменить параметры установки, используйте файл setup.ini.

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

- 2 ГБ свободного места на жестком диске;
- процессор 1 ГГц (с поддержкой инструкций SSE2);
- оперативная память:
  - для 32-разрядной операционной системы – 1 ГБ;
  - для 64-разрядной операционной системы – 2 ГБ.

Поддерживаемые операционные системы для рабочих станций:

- Windows 7 Home / Professional / Enterprise Service Pack 1 и выше;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

Особенности поддержки операционной системы Microsoft Windows 10 вы можете узнать в базе знаний Службы технической поддержки.

Поддерживаемые операционные системы для серверов:

- Windows Small Business Server 2011 Essentials / Standard (64-разрядная);
- Windows MultiPoint Server 2011 (64-разрядная);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
  Windows Server 2019 Essentials / Standard / Datacenter.

Особенности поддержки операционной системы Microsoft Windows Server 2016 и Microsoft Windows Server 2019 вы можете узнать в базе знаний Службы технической поддержки.

Поддерживаемые виртуальные платформы:

- VMware Workstation 15;
- VMware ESXi 6.7 U2;
- Microsoft Hyper-V 2019 Server;
- Citrix Hypervisor 8;
- Citrix XenDesktop 7.18;
- Citrix XenApp 7.18;
- Citrix Provisioning Services 7.18.

Сравнение функций программы в зависимости от типа операционной системы

Набор доступных функций Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready зависит от типа операционной системы: рабочая станция или сервер (см. таблицу ниже).

Сравнение функций Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready

Функция	Рабочая станция	Сервер
Продвинутая защита		
Kaspersky Security Network	✓	✓
Анализ поведения	✓	✓
Защита от эксплойтов	✓	✓
Предотвращение вторжений	✓	–
Откат вредоносных действий	✓	✓
Базовая защита		
Защита от файловых угроз	✓	✓
Защита от веб-угроз	✓	–
Защита от почтовых угроз	✓	–
Сетевой экран	✓	✓
Защита от сетевых угроз	✓	✓
Защита от атак BadUSB	✓	✓

Поставщик AMSI-защиты	✓	✓
Контроль безопасности		
Контроль программ	✓	✓
Контроль устройств	✓	–
Веб-Контроль	✓	–
Адаптивный контроль аномалий	✓	–
Шифрование данных		
Шифрование диска Kaspersky	✓	–
Шифрование диска BitLocker	✓	✓
Шифрование файлов	✓	–
Шифрование съемных дисков	✓	–
Endpoint Agent	✓	✓

Сравнение функций программы в зависимости от инструментов управления

Набор доступных функций Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зависит от инструментов управления (см. таблицу ниже).

Вы можете управлять программой с помощью следующих консолей Kaspersky Security Center:

- Консоль администрирования. Оснастка к Microsoft Management Console (MMC), которая устанавливается на рабочее место администратора.
- Web Console. Компонент Kaspersky Security Center, который устанавливается на Сервер администрирования. Вы можете работать в Web Console через браузер на любом компьютере, который имеет доступ к Серверу администрирования.

Вы также можете управлять программой с помощью Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console – это облачная версия Kaspersky Security Center. То есть Сервер администрирования и другие компоненты Kaspersky Security Center установлены в облачной инфраструктуре "Лаборатории Касперского". Подробнее об управлении программой с помощью Kaspersky Security Center Cloud Console см. в справке Kaspersky Security Center Cloud Console.

Сравнение функций Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready

Функция	Kaspersky Security Center		Kaspersky Security Center
	Консоль администрирования	Web Console	Cloud Console
Продвинутая защита			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Анализ поведения	✓	✓	✓
Защита от эксплойтов	✓	✓	✓
Предотвращение вторжений	✓	✓	✓
Откат вредоносных действий	✓	✓	✓
Базовая защита			
Защита от файловых угроз	✓	✓	✓
Защита от веб-угроз	✓	✓	✓
Защита от почтовых угроз	✓	✓	✓
Сетевой экран	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓
Защита от атак BadUSB	✓	✓	✓
Поставщик AMSI-защиты	✓	✓	✓
Контроль безопасности			
Контроль программ	✓	✓	✓
Контроль устройств	✓	✓	✓
Веб-Контроль	✓	✓	✓
Адаптивный контроль аномалий	✓	✓	–
Шифрование данных			
Шифрование диска Kaspersky	✓	✓	–
Шифрование диска BitLocker	✓	✓	–
Шифрование файлов	✓	✓	–
Шифрование съемных дисков	✓	✓	–

Endpoint Agent	✓	✓	✓
Задачи			
Добавление ключа	✓	✓	✓
Изменение состава компонентов программы	✓	✓	✓
Инвентаризация	✓	✓	✓
Обновление	✓	✓	✓
Откат обновления	✓	✓	✓
Поиск вирусов	✓	✓	✓
Проверка целостности	✓	✓	–
Удаление данных	✓	✓	✓
Управление учетными записями Агента аутентификации	✓	–	–

Совместимость с другими программами "Лаборатории Касперского"

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет компьютер на наличие программ "Лаборатории Касперского" перед установкой.

Программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready несовместима со следующими программами "Лаборатории Касперского":

- Kaspersky Small Oice Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (в том числе компонент Endpoint Sensor).
- Kaspersky Sandbox (в том числе Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (в том числе компонент Endpoint Sensor).

Если на компьютере установлен компонент Endpoint Agent с помощью инструментов развертывания других программ "Лаборатории Касперского", при установке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready компонент будет удален автоматически. При этом

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может включать в себя компонент Endpoint Sensor / Kaspersky Endpoint Agent, если в списке компонентов программы вы выбрали Endpoint Agent.

- Kaspersky Security для виртуальных сред Легкий агент.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security для Windows Server.
- Kaspersky Embedded Systems Security.

Если на компьютере установлены программы "Лаборатории Касперского" из списка, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет эти программы. Дождитесь завершения этого процесса, чтобы продолжить установку Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Установка и удаление программы

Программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready может быть установлена на компьютер следующими способами:

- локально с помощью мастера установки программы.
- локально из командной строки. удаленно с
- помощью Kaspersky Security Center 12.
- удаленно через редактор управления групповыми политиками Microsoft Windows (подробнее см. на сайте Службы технической поддержки Microsoft).
- удаленно с помощью System Center Con guration Manager.

Вы можете настроить параметры установки программы несколькими способами. Если вы одновременно используете несколько способов настройки параметров, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready применяет параметры с наивысшим приоритетом. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready использует следующий порядок приоритетов:

1. Параметры, полученные из файла setup.ini.
2. Параметры, полученные из файла installer.ini.
3. Параметры, полученные из командной строки.

Перед началом установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready (в том числе удаленной) рекомендуется закрыть все работающие программы.

Развертывание через Kaspersky Security Center 12

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready можно разворачивать на компьютерах в сети организации несколькими способами. Вы можете выбрать наиболее подходящий для вашей организации способ развертывания, а также использовать несколько способов развертывания одновременно. Kaspersky Security Center поддерживает следующие основные способы развертывания:

- Установка программы с помощью мастера развертывания защиты.

  Стандартный способ установки, который удобен, если вас удовлетворяют параметры Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready по умолчанию и в вашей организации простая инфраструктура, которая не требует специальной настройки.

- Установка программы с помощью задачи удаленной установки.

  Универсальный способ установки, который позволяет настроить параметры Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и гибко управлять задачами удаленной установки. Установка Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready состоит из следующих этапов:

  1. создание инсталляционного пакета;

2. создание задачи удаленной установки.

Kaspersky Security Center также поддерживает другие способы установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, например, развертывание в составе образа операционной системы. Подробнее о других способах развертывания см. в справке Kaspersky Security Center.

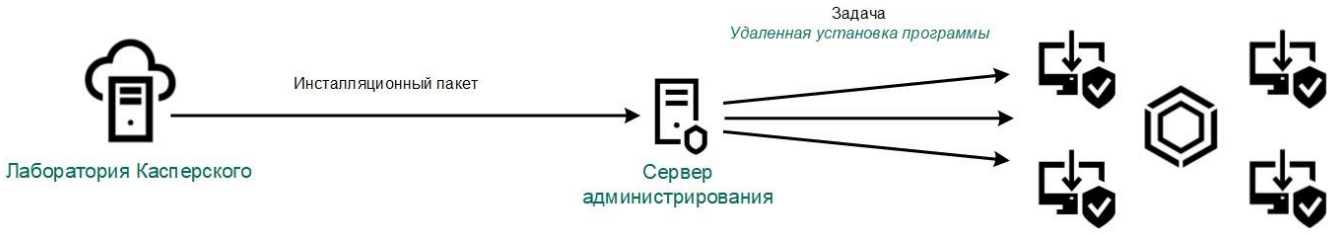
Стандартная установка программы

Для установки программы на компьютерах организации в Kaspersky Security Center предусмотрен мастер развертывания защиты. Мастер развертывания защиты включает в себя следующие основные действия:

1. Выбор инсталляционного пакета Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

   Инсталляционный пакет – набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы. Инсталляционный пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready общий для всех поддерживаемых версий операционной системы Windows и типов архитектуры процессора.

2. Создание задачи Сервера администрирования Kaspersky Security Center Удаленная установка программы.



Развертывание Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready

Как запустить мастер развертывания защиты в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Дополнительно → Удаленная установка.

2. Нажмите на ссылку Развернуть инсталляционный пакет на управляемые устройства (рабочие места).

В результате запустится мастер развертывания защиты. Следуйте его указаниям.

На клиентском компьютере необходимо открыть порты TCP 139 и 445, UDP 137 и 138.

Шаг 1. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если в списке отсутствует инсталляционный пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, вы можете создать пакет в мастере.

Вы можете настроить параметры инсталляционного пакета в Kaspersky Security Center, например, выбрать компоненты программы, которые будут установлены на компьютер.

Также с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет установлен Агент администрирования. Агент администрирования обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Шаг 2 Выбор устройств для установки

Выберите компьютеры, на которые будет установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.

- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. На нераспределенных устройствах не установлен Агент администрирования. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Определение параметров задачи удаленной установки

Настройте следующие дополнительные параметры программы:

- Принудительно загрузить инсталляционный пакет. Выберите средства установки программы:

- С помощью Агента администрирования. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready устанавливается средствами Агента администрирования.

- Средствами операционной системы с помощью точек распространения. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.

- Средствами операционной системы с помощью Сервера администрирования. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

- Поведение устройств, управляемых другими Серверами. Выберите способ установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

- Не устанавливать программу, если она уже установлена. Снимите этот флажок, если вы хотите, например, установить программу более ранней версии.

- Назначить установку Агента администрирования в групповых политиках Active Directory. Установка Агента администрирования средствами Active Directory вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.

Шаг 4. Выбор лицензионного ключа

Добавьте ключ в инсталляционный пакет для активации программы. Этот шаг не является обязательным. Если на Сервере администрирования размещен лицензионный ключ с функцией автоматического распространения, ключ будет добавлен автоматически позднее. Также вы можете активировать программу позднее с помощью задачи Добавить ключ.

Шаг 5. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера. При установке Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые программы. Также перезагрузка может потребоваться при обновлении версии программы.

Шаг 6. Удаление несовместимых программ перед установкой программы

Ознакомьтесь со списком несовместимых программы и разрешите удаление этих программ. Если на компьютере установлены несовместимые программы, установка Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready завершается с ошибкой.

Шаг 7. Выбор учетной записи для доступа к устройствам

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 8. Запуск установки

Завершите работу мастера. Если требуется, установите флажок Не запустить задачу после завершения работы мастера удаленной установки. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как запустить мастер развертывания защиты в Web Console и Cloud Console

В главном окне Web Console выберите Обнаружение устройств и развертывание → Развертывание и назначение → Мастер развертывания защиты.

В результате запустится мастер развертывания защиты. Следуйте его указаниям.

На клиентском компьютере необходимо открыть порты TCP 139 и 445, UDP 137 и 138.

Шаг 1. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если в списке отсутствует инсталляционный пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, вы можете создать пакет в мастере. Для создания инсталляционного пакета вам не нужно искать дистрибутив и сохранять его в память компьютера. В Kaspersky Security Center доступен список дистрибутивов, размещенных на серверах "Лаборатории Касперского", и создание инсталляционного пакета выполняется автоматически. "Лаборатория Касперского" обновляет список после выпуска новых версий программ.

Вы можете настроить параметры инсталляционного пакета в Kaspersky Security Center, например, выбрать компоненты программы, которые будут установлены на компьютер.

Шаг 2. Выбор лицензионного ключа

Добавьте ключ в инсталляционный пакет для активации программы. Этот шаг не является обязательным. Если на Сервере администрирования размещен лицензионный ключ с функцией автоматического распространения, ключ будет добавлен автоматически позднее. Также вы можете активировать программу позднее с помощью задачи Добавить ключ.

Шаг 3. Выбор Агента администрирования

Выберите версию Агента администрирования, который будет установлен вместе с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Агент администрирования обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Шаг 4. Выбор устройств для установки

Выберите компьютеры, на которые будет установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. На нераспределенных устройствах не установлен Агент администрирования. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 5. Настройка дополнительных параметров

Настройте следующие дополнительные параметры программы:

- Принудительно загрузить инсталляционный пакет. Выбор средства установки программы:

- С помощью Агента администрирования. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready устанавливается средствами Агента администрирования.

- Средствами операционной системы с помощью точек распространения. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.

- Средствами операционной системы с помощью Сервера администрирования. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

- Не устанавливать программу, если она уже установлена. Снимите этот флажок, если вы хотите, например, установить программу более ранней версии.

- Назначить установку инсталляционного пакета в групповых политиках Active Directory. Установка Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready выполняется средствами Агента администрирования или средствами Active Directory вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.

Шаг 6. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера. При установке Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые программы. Также перезагрузка может потребоваться при обновлении версии программы.

Шаг 7. Удаление несовместимых программ перед установкой программы

Ознакомьтесь со списком несовместимых программы и разрешите удаление этих программ. Если на компьютере установлены несовместимые программы, установка Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready завершается с ошибкой.

Шаг 8. Перемещение в группу администрирования

Выберите группу администрирования, в которую будут перемещены компьютеры после установки Агента администрирования. Перемещение в группу администрирования необходимо для применения политик и групповых задач. Если компьютер уже состоит в любой группе

администрирования, то компьютер перемещен не будет. Если вы не выберете группу администрирования, компьютеры будут добавлены в группу Нераспределенные устройства.

Шаг 9. Выбор учетной записи для доступа к устройствам

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 10. Запуск установки

Завершите работу мастера. Если требуется, установите флажок Запустить задачу после завершения работы мастера. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Создание инсталляционного пакета

Инсталляционный пакет – набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы. Инсталляционный пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready общий для всех поддерживаемых версий операционной системы Windows и типов архитектуры процессора.

Как создать инсталляционный пакет в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.

2. Нажмите на кнопку Создать инсталляционный пакет.

   Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

Шаг 1. Выбор типа инсталляционного пакета

Выберите вариант Создать инсталляционный пакет для программы "Лаборатории Касперского".

Шаг 2. Определение имени инсталляционного пакета

Введите имя инсталляционного пакета, например, `Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.4.0`.

Шаг 3. Выбор дистрибутива программы для установки

Нажмите на кнопку Обзор и выберите файл `kes_win.kud`, который входит в комплект поставки.

Если требуется, обновите антивирусные базы в инсталляционном пакете с помощью флажка Скопировать обновления из хранилища в инсталляционный пакет.

Шаг 4. Лицензионное соглашение и Политика конфиденциальности

Прочитайте и примите условия Лицензионного соглашения и Политики конфиденциальности.

Инсталляционный пакет будет создан и добавлен в Kaspersky Security Center. С помощью инсталляционного пакета вы можете установить Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на компьютеры сети организации или обновить версию программы. Также в параметрах инсталляционного пакета вы можете выбрать компоненты программы и настроить параметры установки программы (см. таблицу ниже). Инсталляционный пакет содержит антивирусные базы из хранилища Сервера администрирования. Вы можете обновлять базы в инсталляционном пакете, чтобы уменьшить расход трафика при обновлении баз после установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Как создать инсталляционный пакет в Web Console и Cloud Console

1. В главном окне Web Console выберите Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.

2. Нажмите на кнопку Добавить.

   Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

Шаг 1. Выбор типа инсталляционного пакета

Выберите вариант Создать инсталляционный пакет для программы "Лаборатории Касперского".

Мастер создаст инсталляционный пакет из дистрибутива, размещенного на серверах "Лаборатории Касперского". Список обновляется автоматически по мере выпуска новых версий программ. Для установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready рекомендуется выбрать этот вариант.

Также вы можете создать инсталляционный пакет из файла.

Шаг 2. Инсталляционные пакеты

Выберите инсталляционный пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows. Запустится процесс создания инсталляционного пакета. Во время создания инсталляционного пакета необходимо принять условия Лицензионного соглашения и Политики конфиденциальности.

Инсталляционный пакет будет создан и добавлен в Kaspersky Security Center. С помощью инсталляционного пакета вы можете установить Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на компьютеры сети организации или обновить версию программы. Также в параметрах инсталляционного пакета вы можете выбрать компоненты программы и настроить параметры установки программы (см. таблицу ниже). Инсталляционный пакет содержит антивирусные базы из хранилища Сервера администрирования. Вы можете обновлять базы в инсталляционном пакете, чтобы уменьшить расход трафика при обновлении баз после установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Параметры инсталляционного пакета

Раздел	Описание
Компоненты защиты	В этом разделе вы можете выбрать компоненты программы, которые будут доступны. Вы можете изменить состав компонентов программы позднее с помощью задачи Изменение состава компонентов программы. Компоненты Защита от атак BadUSB, Endpoint Agent и компоненты шифрования данных не устанавливаются по умолчанию. Эти компоненты можно добавить только в параметрах инсталляционного пакета.

Параметры установки	Добавить путь к программе в переменную окружения %PATH%. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки. Не защищать процесс установки программы. Защита установки включает в себя защиту от подмены дистрибутива вредоносными программами, блокирование доступа к папке установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и блокирование доступа к разделу системного реестра с ключами программы. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop). Обеспечить совместимость с Citrix PVS. Вы можете включить поддержку Citrix Provisioning Services для установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready на виртуальную машину. Путь к папке для установки программы. Вы можете изменить путь установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready на клиентском компьютере. По умолчанию программа устанавливается в папку `%ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready for Windows`. Конфигурационный файл. Вы можете загрузить файл, который задает параметры работы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Вы можете создать конфигурационный файл в локальном интерфейсе программы.

Обновление баз в инсталляционном пакете

Инсталляционный пакет содержит антивирусные базы из хранилища Сервера администрирования, актуальные при создании инсталляционного пакета. После создания инсталляционного пакета вы можете обновлять антивирусные базы в инсталляционном пакете. Это позволяет уменьшить расход трафика на обновление антивирусных баз после установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

Чтобы обновить антивирусные базы в хранилище Сервера администрирования, используйте задачу Сервера администрирования Загрузка обновлений в хранилище Сервера администрирования. Подробнее об обновлении антивирусных баз в хранилище Сервера администрирования см. в справке Kaspersky Security Center.

Вы можете обновлять базы в инсталляционном пакете только в Консоли администрирования и Kaspersky Security Center Web Console. Обновлять базы в инсталляционном пакете в программе Kaspersky Security Center Cloud Console невозможно.

Как обновить антивирусные базы в инсталляционном пакете через Консоль администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты.

Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.

2. Откройте свойства инсталляционного пакета.

3. В разделе Общие нажмите на кнопку Обновить базы.

В результате антивирусные базы в инсталляционном пакете будут обновлены из хранилища Сервера администрирования. Файл `bases.cab`, который входит в комплект поставки, будет заменен папкой `bases`. Внутри папки будут расположены файлы пакетов обновлений.

Как обновить антивирусные базы в инсталляционном пакете через Web Console

1. В главном окне Web Console выберите Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты.

Откроется список инсталляционных пакетов, загруженных в Web Console.

2. Нажмите на название инсталляционного пакета Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, в котором вы хотите обновить антивирусные базы.

Откроется окно свойств инсталляционного пакета.

3. На закладке Общая информация нажмите на ссылку Обновить базы.

В результате антивирусные базы в инсталляционном пакете будут обновлены из хранилища Сервера администрирования. Файл `bases.cab`, который входит в комплект поставки, будет заменен папкой `bases`. Внутри папки будут расположены файлы пакетов обновлений.

Создание задачи удаленной установки

Для удаленной установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предназначена задача Удаленная установка программы. Задача Удаленная установка программы позволяет развернуть инсталляционный пакет программы на все компьютеры организации. Перед развертыванием инсталляционного пакета вы можете обновить антивирусные базы внутри пакета, а также выбрать доступные компоненты программы в свойствах инсталляционного пакета.

Как создать задачу удаленной установки в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Новая задача.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите Сервер администрирования Kaspersky Security Center → Удаленная установка программы.

Шаг 2. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если в списке отсутствует инсталляционный пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, вы можете создать пакет в мастере.

Вы можете настроить параметры инсталляционного пакета в Kaspersky Security Center, например, выбрать компоненты программы, которые будут установлены на компьютер.

Также с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет установлен Агент администрирования. Агент администрирования обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Шаг 3. Дополнительно

Выберите инсталляционный пакет Агента администрирования. Выбранная версия Агента администрирования будет установлена вместе с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Шаг 4. Параметры

Настройте следующие дополнительные параметры программы:

- Принудительно загрузить инсталляционный пакет. Выберите средства установки программы:

- С помощью Агента администрирования. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready устанавливается средствами Агента администрирования.

- Средствами операционной системы с помощью точек распространения. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.

- Средствами операционной системы с помощью Сервера администрирования. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском

компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

- Поведение устройств, управляемых другими Серверами. Выберите способ установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

- Не устанавливать программу, если она уже установлена. Снимите этот флажок, если вы хотите, например, установить программу более ранней версии.

Шаг 5. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера. При установке Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые программы. Также перезагрузка может потребоваться при обновлении версии программы.

Шаг 6. Выбор устройств, которым будет назначено задача

Выберите компьютеры, на которые будет установлена программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.

- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. На нераспределенных устройствах не установлен Агент администрирования. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 7. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 8. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 9. Определение названия задачи

Введите название задачи, например, `Установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.4.0`

Шаг 10. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок Запустить задачу после завершения работы мастера. Вы можете следить за ходом выполнения задачи в свойствах задачи. Установка программы будет выполнена в тихом режиме. После установки в области уведомлений компьютера пользователя будет добавлен значок . Если значок имеет вид , убедитесь, что вы активировали программу.

Как создать задачу удаленной установки в Web Console и Cloud Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Добавить.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающимся списке Программа выберите Kaspersky Security Center.
2. В раскрывающемся списке Тип задачи выберите Удаленная установка программы.
3. В поле Название задачи введите короткое описание, например, `Установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для менеджеров`.
4. В блоке Устройства, которым будет назначена задача выберите область действия задачи.

Шаг 2. Выбор компьютеров для установки

На этом шаге выберите компьютеры, на которые будет установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, в соответствии с выбранным вариантом области действия задачи.

Шаг 3. Настройка параметров инсталляционного пакета

На этом шаге настройте параметры инсталляционного пакета:

1. Выберите инсталляционный пакет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).
2. Выберите инсталляционный пакет Агента администрирования.

   Выбранная версия Агента администрирования будет установлена вместе с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Агент администрирования обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

3. В блоке Принудительно загружать инсталляционный пакет выберите средства установки программы:

   - С помощью Агента администрирования. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready устанавливается средствами Агента администрирования.

- Средствами операционной системы с помощью точек распространения. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.

- Средствами операционной системы с помощью Сервера администрирования. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

4. В поле Максимальное количество одновременных загрузок установите ограничение количества запросов к Серверу администрирования для загрузки инсталляционного пакета. Ограничение запросов позволит избежать перегрузки сети.

5. В поле Количество попыток установки установите ограничение попыток установить программу. Если установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready завершается с ошибкой, задача автоматически запускает установку повторно.

6. Если требуется, снимите флажок Не устанавливать программу, если она уже установлена. Это позволит, например, установить программу более ранней версии.

7. Если требуется, снимите флажок Предварительно проверять версию операционной системы. Это позволит избежать загрузки дистрибутива программы, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютера соответствует программным требованиям, проверку можно пропустить.

8. Если требуется, установите флажок Назначить установку инсталляционного пакета в групповых политиках Active Directory. Установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняется средствами Агента администрирования или средствами Active Directory вручную. Для установки Агента
администрирования задача удаленной установки должна быть запущена с правами администратора домена.

9. Если требуется, установите флажок Предлагать пользователю закрыть работающие программы. Установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready требует ресурсов компьютера. Для удобства пользователя мастер установки программы предлагает закрыть работающие программы перед началом установки. Это позволит избежать замедление в работе других программ и возможных сбоев в работе компьютера.

10. В блоке Поведение устройств, управляемых этим Сервером выберите способ установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

Шаг 4. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 5. Завершение создания задачи

Завершите работу мастера по кнопке Готово. В списке задач отобразится новая задача. Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку Запустить. Установка программы будет выполнена в тихом режиме. После установки в области уведомлений компьютера пользователя будет добавлен значок . Если значок имеет вид , убедитесь, что вы активировали программу.

Локальная установка программы с помощью мастера

Интерфейс мастера установки программы состоит из последовательности окон, соответствующих шагам установки программы.

Чтобы установить программу или обновить предыдущую версию программы с помощью мастера установки программы,

скопируйте файл setup_kes.exe, входящий в комплект поставки, на компьютер пользователя и запустите его.

Запустится мастер установки программы.

Подготовка к установке

Перед установкой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready на компьютер или обновлением предыдущей версии программы проверяются следующие условия:

- наличие несовместимого программного обеспечения (список несовместимого ПО приведен в файле incompatible.txt в комплекте поставки); выполнение аппаратных и программных требований;
- наличие прав на установку программного обеспечения.

Если какое-либо из перечисленных условий не выполнено, на экран выводится соответствующее уведомление.

Если компьютер соответствует предъявляемым требованиям, мастер установки программы выполняет поиск программ "Лаборатории Касперского", одновременная работа которых может привести к возникновению конфликтов. Если такие программы найдены, вам предлагается удалить их вручную.

Если в числе обнаруженных программ есть предыдущие версии Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, то все данные, которые могут быть мигрированы (например, информация об активации, параметры программы), сохраняются и используются при установке Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready 11.4.0 для Windows, а предыдущая версия программы автоматически удаляется. Это относится к следующим версиям программы:

- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready 10 Service Pack 1 Maintenance Release 4 для Windows (сборка 10.2.6.3733).
- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready 10 Service Pack 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready 10 Service Pack 2 Maintenance Release 1 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready 10 Service Pack 2 Maintenance Release 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready 10 Service Pack 2 Maintenance Release 3 для Windows (сборка 10.3.3.275).
- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready 10 Service Pack 2 Maintenance Release 4 для Windows (сборка 10.3.3.275).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.0.0 (сборка 11.0.0.6499).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.0.1 (сборка 11.0.1.90).

- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.1.0 (сборка 11.1.0.15919).
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.1.1 (сборка 11.1.1.126).
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.2.0 (сборка 11.2.0.2254).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.3.0 (сборка 11.3.0.773).

Компоненты Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready

В процессе установки вы можете выбрать компоненты Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, которые вы хотите установить. Компонент Защита от файловых угроз является обязательным компонентом для установки. Вы не можете отменить его установку.

По умолчанию для установки выбраны все компоненты программы, кроме следующих компонентов:

- Защита от атак BadUSB.
- Шифрование файлов.
- Полнодисковое шифрование.
- Управление BitLocker.
- Endpoint Agent. Endpoint Agent устанавливает программу Kaspersky Endpoint Agent для взаимодействие между программой и решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, Kaspersky Sandbox).

Вы можете изменить состав компонентов после установки программы. Для этого вам нужно запустить мастер установки повторно и выбрать операцию изменения состава компонентов.

Дополнительные параметры

Защитить процесс установки программы. Защита установки включает в себя защиту от подмены дистрибутива вредоносными программами, блокирование доступа к папке установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и блокирование доступа к разделу системного реестра с ключами программы. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).

Обеспечить совместимость с Citrix PVS. Вы можете включить поддержку Citrix Provisioning Services для установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на виртуальную машину.

Добавить путь к программе в переменную окружения %PATH%. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки.

Установка программы из командной строки

Установку Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки программы.
- В тихом режиме. После запуска установки в тихом режиме ваше участие в процессе установки не требуется. Для установки программы в тихом режиме используйте ключи `/s` и `/qn`.

> Перед установкой программы в тихом режиме откройте и прочитайте Лицензионное соглашение и текст Политики конфиденциальности. Лицензионное соглашение и текст Политики конфиденциальности входят в комплект поставки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Приступайте к установке программы, только если вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения, если вы понимаете и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности, если вы полностью прочитали и понимаете Политику конфиденциальности. Если вы не принимаете положения и условия Лицензионного соглашения и Политику конфиденциальности, не устанавливайте и не используйте Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

Чтобы установить программу или обновить предыдущую версию программы, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.
3. Выполните команду:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1|0]
[/pSKIPPRODUCTCHECK=1|0]  [/pSKIPPRODUCTUNINSTALL=1|0]  [/pKLLOGIN=<имя  пользователя>
/pKLPASSWD=<пароль> /pKLPASSWDAREA=<область действия пароля>] [/pENABLETRACES=1|0
/pTRACESLEVEL=<уровень трассировки>] [/s] или
msiexec /i <название дистрибутива> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1|0]  [SKIPPRODUCTCHECK=1|0]  [SKIPPRODUCTUNINSTALL=1|0]  [KLLOGIN=<имя
пользователя> KLPASSWD=<пароль> KLPASSWDAREA=<область действия пароля>]
[ENABLETRACES=1|0 TRACESLEVEL=<уровень трассировки>] [/qn]
```

EULA=1	Согласие с положениями Лицензионного соглашения. Текст Лицензионного соглашения входит в комплект поставки Kaspersky Endpoint Security. Согласие с положениями Лицензионного соглашения является необходимым условием для установки программы или обновления версии программы.
PRIVACYPOLICY=1	Согласие с Политикой конфиденциальности. Текст Политики конфиденциальности входит в комплект поставки Kaspersky Endpoint Security. Согласие с Политикой конфиденциальности является необходимым условием для установки программы или обновления версии программы.
KSN	Согласие или отказ участвовать в Kaspersky Security Network (KSN). Если параметр не указан, Kaspersky Endpoint Security запросит подтверждения участия в KSN при первом запуске программы. Возможные значения: • 1 – согласие участвовать в KSN. • 0 – отказ участвовать в KSN (значение по умолчанию). Дистрибутив Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready оптимизирован для использования Kaspersky Security Network. Если вы отказались от участия в Kaspersky Security Network, то сразу после завершения установки обновите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
ALLOWREBOOT=1	Автоматическая перезагрузка компьютера после установки или обновления программы, если требуется. Если параметр не задан, автоматическая перезагрузка компьютера запрещена. При установке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые программы. Также перезагрузка может потребоваться при обновлении версии программы.
SKIPPRODUCTCHECK=1	Выключение проверки на наличие несовместимого ПО. Список несовместимого ПО приведен в файле incompatible.txt в комплекте поставки. Если параметр не задан, при обнаружении несовместимого ПО установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет прекращена.

SKIPPRODUCTUNINSTALL=1	Запрет на автоматическое удаление найденного несовместимого ПО. Если параметр не задан, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready пытается удалить несовместимое ПО.
KLLOGIN	Установка имени пользователя для доступа к управлению функциями и параметрами Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (компонент Защита паролем). Имя пользователя устанавливается вместе с параметрами KLPASSWD и KLPASSWDAREA. По умолчанию используется имя пользователя KLAdmin.
KLPASSWD	Установка пароля для доступа к управлению функциями и параметрами Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (пароль устанавливается вместе с параметрами KLLOGIN и KLPASSWDAREA). Если вы указали пароль, но не задали имя пользователя с помощью параметра KLLOGIN, то по умолчанию используется имя пользователя KLAdmin.
KLPASSWDAREA	Определение области действия пароля для доступа к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. При попытке пользователя выполнить действие из этой области Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запрашивает учетные данные пользователя (параметры KLLOGIN и KLPASSWD). Для указания множественного значения используйте символ ";". Возможные значения: • SET – изменение параметров программы. • EXIT – завершение работы программы. • DISPROTECT – выключение компонентов защиты и остановка задач проверки. • DISPOLICY – выключение политики Kaspersky Security Center. • UNINST – удаление программы с компьютера.
	• DISCTRL – выключение компонентов контроля. • REMOVELIC – удаление ключа. • REPORTS – просмотр отчетов.
ENABLETRACES	Включение или выключение трассировки программы. После запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready программа сохраняет файлы трассировки в папке %ProgramData%/Kaspersky Lab. Возможные значения: • 1 – трассировка включена. • 0 – трассировка выключена (значение по умолчанию).

TRACESLEVEL	Уровень детализации трассировки. Возможные значения: • 100 (критический). Только сообщения о неустранимых ошибках. • 200 (высокий). Сообщения о всех ошибках, включая неустранимые. • 300 (диагностический). Сообщения о всех ошибках, а также предупреждения. • 400 (важный). Сообщения о всех ошибках, предупреждения, а также дополнительная информация. • 500 (обычный). Сообщения о всех ошибках, предупреждениях, а также подробная информация о работе программы в нормальном режиме (значение по умолчанию). • 600 (низкий). Все сообщения.
AMPPL	Включение или выключение защиты процессов Kaspersky Endpoint Security с использованием технологии AM-PPL (Antimalware Protected Process Light). Подробнее о технологии AM-PPL см. на сайте Microsoft. Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019. Возможные значения: • 1 – защита процессов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с использованием технологии AM-PPL включена (значение по умолчанию). • 0 – защита процессов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с использованием технологии AM-PPL выключена.
RESTAPI	Управление программой через REST API. Для управления программой через REST API обязательно нужно задать имя пользователя (параметр RESTAPI_User). Возможные значения: • 1 – управление через REST API разрешено. • 0 – управление через REST API запрещено (значение по умолчанию). Для управления программой через REST API должно быть разрешено управление с помощью систем администрирования. Для этого задайте параметр AdminKitConnector=1. Если вы управляете программой через REST API, управлять программой с помощью систем администрирования "Лаборатории Касперского" невозможно.

RESTAPI_User	Имя пользователя доменной учетной записи Windows для управления программой через REST API. Управление программой через REST API доступно только этому пользователю. Введите имя пользователя в формате <DOMAIN>\<UserName> (например, RESTAPI_User=COMPANY\Administrator). Для работы с REST API вы можете выбрать только одного пользователя. Добавление имени пользователя является необходимым условием для управления программой через REST API.
RESTAPI_Port	Порт для управления программой через REST API. По умолчанию используется порт 6782.
ADMINKITCONNECTOR	Управление программой с помощью систем администрирования. К системам администрирования относится, например, Kaspersky Security Center. Кроме систем администрирования "Лаборатории Касперского" вы можете использовать сторонние решения. Для этого Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предоставляет API. Возможные значения: • 1 – управление программой с помощью систем администрирования разрешено (значение по умолчанию). • 0 – разрешено управление программой только через локальный интерфейс.

Пример:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 msiexec /i kes_win.msi EULA=1
PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn setup_kes.exe
/pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

После установки программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready происходит активация по пробной лицензии, если вы не указали код активации в файле setup.ini. Пробная лицензия обычно имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно активировать программу по коммерческой лицензии с помощью мастера активации программы или специальной команды.

Во время установки программы или обновления версии программы в тихом режиме поддерживается использование следующих файлов:

- setup.ini – общие параметры установки программы;
- install.cfg – параметры работы Kaspersky Endpoint

Security для бизнеса - Расширенный EDR Ready; • setup.reg

– ключи реестра.

Запись ключей реестра из файла setup.reg в реестр осуществляется, только если в файле setup.ini указано значение `setup.reg` для параметра `SetupReg`. Файл setup.reg формируется специалистами "Лаборатории Касперского". Не рекомендуется изменять содержимое этого файла.

Чтобы применить параметры из файлов setup.ini, install.cfg и setup.reg, разместите эти файлы в папке с дистрибутивом Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Удаленная установка программы с помощью System Center Con guration Manager

Инструкция актуальна для версии System Center Con guration Manager 2012 R2.

Чтобы удаленно установить программу с помощью System Center Con guration Manager, выполните следующие действия:

1. Откройте консоль Con guration Manager.
2. В правой части консоли в блоке Управление приложениями выберите раздел Пакеты.
3. В верхней части консоли в панели управления нажмите на кнопку Создать пакет.

   Запустится мастер создания пакетов и программ.
4. В мастере создания пакетов и программ выполните следующие действия:

   a. В разделе Пакет выполните следующие действия:

   - В поле Имя введите имя инсталляционного пакета.
   - В поле Исходная папка укажите путь к папке, в которой расположен дистрибутив Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

   b. В разделе Тип программы выберите вариант Стандартная программа.

   c. В разделе Стандартная программа выполните следующие действия:

   - В поле Имя введите уникальное имя инсталляционного пакета (например, название программы с указанием версии).
   - В поле Командная строка укажите параметры установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из командной строки.
   - По кнопке Обзор задайте путь к исполняемому файлу программы.
   - Убедитесь, что в раскрывающемся списке Режим выполнения выбран элемент Запустить с правами администратора.

   d. В разделе Требования выполните следующие действия:

- Установите флажок Запустить сначала другую программу, если вы хотите, чтобы перед установкой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready была запущена другая программа.

  Выберите программу из раскрывающегося списка Программа или укажите путь к исполняемому файлу этой программы по кнопке Обзор.

- Выберите вариант Эту программу можно запускать только на указанных платформах в блоке Требования к платформе, если вы хотите, чтобы программа была установлена только в указанных операционных системах.

  В списке ниже установите флажки напротив тех операционных систем, в которых должен быть установлен Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Этот шаг является необязательным.

e. В разделе Сводка проверьте все заданные значения параметров и нажмите на кнопку Далее.

Созданный инсталляционный пакет появится в разделе Пакеты в списке доступных инсталляционных пакетов.

5. В контекстном меню инсталляционного пакета выберите пункт Развернуть.

   Запустится мастер развертывания программного обеспечения.

6. В мастере развертывания программного обеспечения выполните следующие действия:

   a. В разделе Общие выполните следующие действия:

   - В поле Программное обеспечение введите уникальное имя инсталляционного пакета или выберите инсталляционный пакет из списка по кнопке Обзор.

   - В поле Коллекция введите название коллекции компьютеров, на которые должна быть установлена программа, или выберите эту коллекцию по кнопке Обзор.

   b. В разделе Содержимое добавьте точки распространения (более подробную информацию вы можете найти в сопроводительной документации для System Center Con guration Manager).

   c. Если требуется, укажите значения других параметров в мастере развертывания программного обеспечения. Эти параметры являются необязательными для удаленной установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

   d. В разделе Сводка проверьте все заданные значения параметров и нажмите на кнопку Далее.

После завершения работы мастера развертывания программного обеспечения будет создана задача по удаленной установке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Описание параметров установки в файле setup.ini

Файл setup.ini используется при установке программы из командной строки или с помощью редактора управления групповыми политиками Microsoft Windows. Чтобы применить параметры из файла setup.ini, разместите файл в папке с дистрибутивом Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

ЗАГРУЗИТЬ ФАЙЛ SETUP.INI

Файл setup.ini состоит из следующих разделов:

- `[Setup]` – общие параметры установки программы.
- `[Components]` – выбор компонентов программы для установки. Если не указан ни один из компонентов, то устанавливаются все доступные для операционной системы компоненты. Защита от файловых угроз является обязательным компонентом и устанавливается на компьютер независимо от того, какие параметры указаны в этом блоке.
- `[Tasks]` – выбор задач для включения в список задач Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если не указана ни одна задача, все задачи включаются в список задач Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Вместо значения `1` могут использоваться значения `yes`, `on`, `enable`, `enabled`.

Вместо значения `0` могут использоваться значения `no`, `off`, `disable`, `disabled`.

Параметры файла setup.ini

Раздел	Параметр	Описание
`[Setup]`	`InstallDir`	Путь к папке установки программы.
	`ActivationCode`	Код активации Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
	`EULA=1`	Согласие с положениями Лицензионного соглашения. Текст Лицензионного соглашения входит в комплект поставки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Согласие с положениями Лицензионного соглашения является необходимым условием для установки программы или обновления версии программы.
	`PrivacyPolicy=1`	Согласие с Политикой конфиденциальности. Текст Политики конфиденциальности входит в комплект поставки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Согласие с Политикой конфиденциальности является необходимым условием для установки программы или обновления версии программы.

	KSN	Согласие или отказ участвовать в Kaspersky Security Network (KSN). Если параметр не указан, Kaspersky Endpoint Security запросит подтверждения участия в KSN при первом запуске программы. Возможные значения: • 1 – согласие участвовать в KSN. • 0 – отказ участвовать в KSN (значение по умолчанию).
		Дистрибутив Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready оптимизирован для использования Kaspersky Security Network. Если вы отказались от участия в Kaspersky Security Network, то сразу после завершения установки обновите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
	Login	Установка имени пользователя для доступа к управлению функциями и параметрами Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (компонент Защита паролем). Имя пользователя устанавливается вместе с параметрами Password и PasswordArea. По умолчанию используется имя пользователя KLAdmin.
	Password	Установка пароля для доступа к управлению функциями и параметрами Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (пароль устанавливается вместе с параметрами Login и PasswordArea). Если вы указали пароль, но не задали имя пользователя с помощью параметра Login, то по умолчанию используется имя пользователя KLAdmin.

	PasswordArea	Определение области действия пароля для доступа к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. При попытке пользователя выполнить действие из этой области Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запрашивает учетные данные пользователя (параметры Login и Password). Для указания множественного значения используйте символ ";". Возможные значения: • SET – изменение параметров программы. • EXIT – завершение работы программы. • DISPROTECT – выключение компонентов защиты и остановка задач проверки. • DISPOLICY – выключение политики Kaspersky Security Center. • UNINST – удаление программы с компьютера. • DISCTRL – выключение компонентов контроля. • REMOVELIC – удаление ключа. • REPORTS – просмотр отчетов.
	SelfProtection	Включение или выключение механизма защиты установки программы. Возможные значения: • 1 – механизм защиты установки программы включен (значение по умолчанию). • 0 – механизм защиты установки программы выключен. Защита установки включает в себя защиту от подмены дистрибутива вредоносными программами, блокирование доступа к папке установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и блокирование доступа к разделу системного реестра с ключами программы. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).

	`Reboot=1`	Автоматическая перезагрузка компьютера после установки или обновления программы, если требуется. Если параметр не задан, автоматическая перезагрузка компьютера запрещена. При установке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые программы. Также перезагрузка может потребоваться при обновлении версии программы.
	`AddEnvironment`	Добавление в системную переменную %PATH% пути к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Возможные значения: • `1` – в системную переменную %PATH% добавляется путь к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. • `0` – в системную переменную %PATH% не добавляется путь к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
	`AMPPL`	Включение или выключение защиты процессов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с использованием технологии AM-PPL (Antimalware Protected Process Light). Подробнее о технологии AM-PPL см. на сайте Microsoft. Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019. Возможные значения: • `1` – защита процессов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с использованием технологии AM-PPL включена (значение по умолчанию). • `0` – защита процессов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с использованием технологии AM-PPL выключена.
	`SetupReg`	Включение записи ключей реестра из файла setup.reg в реестр. Значение параметра `SetupReg: setup.reg`.
	`EnableTraces`	Включение или выключение трассировки программы.

		После запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready программа сохраняет файлы трассировки в папке %ProgramData%/Kaspersky Lab. Возможные значения: • `1` – трассировка включена. • `0` – трассировка выключена (значение по умолчанию).
	`TracesLevel`	Уровень детализации трассировки. Возможные значения: • `100` (критический). Только сообщения о неустранимых ошибках. • `200` (высокий). Сообщения о всех ошибках, включая неустранимые. • `300` (диагностический). Сообщения о всех ошибках, а также предупреждения. • `400` (важный). Сообщения о всех ошибках, предупреждения, а также дополнительная информация. • `500` (обычный). Сообщения о всех ошибках, предупреждениях, а также подробная информация о работе программы в нормальном режиме (значение по умолчанию). • `600` (низкий). Все сообщения.
	`RESTAPI`	Управление программой через REST API. Для управления программой через REST API обязательно нужно задать имя пользователя (параметр `RESTAPI_User`). Возможные значения: • `1` – управление через REST API разрешено. • `0` – управление через REST API запрещено (значение по умолчанию). Для управления программой через REST API должно быть разрешено управление с помощью систем администрирования. Для этого задайте параметр `AdminKitConnector=1`. Если вы управляете программой через REST API, управлять программой с помощью систем администрирования "Лаборатории Касперского" невозможно.

	RESTAPI_User	Имя пользователя доменной учетной записи Windows для управления программой через REST API. Управление программой через REST API доступно только этому пользователю. Введите имя пользователя в формате <DOMAIN>\<UserName> (например, RESTAPI_User=COMPANY\Administrator). Для работы с REST API вы можете выбрать только одного пользователя. Добавление имени пользователя является необходимым условием для управления программой через REST API.
	RESTAPI_Port	Порт для управления программой через REST API. По умолчанию используется порт 6782.
[Components]	ALL	Установка всех компонентов. Если указано значение параметра 1, все компоненты будут установлены независимо от параметров установки отдельных компонентов.
	MailThreatProtection	Защита от почтовых угроз.
	WebThreatProtection	Защита от веб-угроз.
	AMSI	Поставщик AMSI-защиты.
	HostIntrusionPrevention	Предотвращение вторжений.
	BehaviorDetection	Анализ поведения.
	ExploitPrevention	Защита от эксплойтов.
	RemediationEngine	Откат вредоносных действий.
	Firewall	Сетевой экран.
	NetworkThreatProtection	Защита от сетевых угроз.
	WebControl	Веб-Контроль.
	DeviceControl	Контроль устройств.
	ApplicationControl	Контроль программ.
	AdaptiveAnomaliesControl	Адаптивный контроль аномалий.
	FileEncryption	Библиотеки для шифрования файлов.
	DiskEncryption	Библиотеки для полнодискового шифрования.
	BadUSBAttackPrevention	Защита от атак BadUSB.

	AntiAPT	Endpoint Agent. Endpoint Agent устанавливает программу Kaspersky Endpoint Agent для взаимодействие между программой и решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, Kaspersky Sandbox).
	AdminKitConnector	Управление программой с помощью систем администрирования. К системам администрирования относится, например, Kaspersky Security Center. Кроме систем администрирования "Лаборатории Касперского" вы можете использовать сторонние решения. Для этого Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предоставляет API. Возможные значения: • 1 – управление программой с помощью систем администрирования разрешено (значение по умолчанию). • 0 – разрешено управление программой только через локальный интерфейс.
[Tasks]	ScanMyComputer	Задача полной проверки. Возможные значения: • 1 – задача включается в список задач Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. • 0 – задача не включается в список задач Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
	ScanCritical	Задача проверки важных областей. Возможные значения: • 1 – задача включается в список задач Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. • 0 – задача не включается в список задач Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
	Updater	Задача обновления. Возможные значения: • 1 – задача включается в список задач Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. • 0 – задача не включается в список задач Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Изменение состава компонентов программы

Во время установки программы вы можете выбрать компоненты, которые будут доступны. Вы можете изменить состав программы следующими способами:

- Локально с помощью мастера установки программы.

  Изменение состава программы выполняется обычным способом, принятым для операционной системы Windows, через Панель управления. Запустите мастер установки программы и выберите операцию изменения состава компонентов программы. Следуйте указаниям на экране.

- Удаленно с помощью Kaspersky Security Center.

  Для изменения состава компонентов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready после установки программы предназначена задача Изменение состава компонентов программы.

Изменение состава программы имеет следующие особенности:

- На компьютеры под управлением Windows Server можно установить не все компоненты Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (например, недоступен компонент Адаптивный контроль аномалий).

- Если на компьютере жесткие диски защищены полнодисковым шифрованием (FDE), удалить компонент Полнодисковое шифрование невозможно. Для удаления компонента Полнодисковое шифрование расшифруйте все жесткие диски компьютера.

- Если на компьютере есть зашифрованные файлы (FLE) или пользователь использует зашифрованные съемные диски (FDE или FLE), после удаления компонентов шифрования данных получить доступ к файлам и съемным дискам будет невозможно. Вы можете получить доступ к файлам и съемным дискам, если переустановите компоненты шифрования данных.

Как добавить или удалить компоненты программы в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Новая задача.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0) → Изменение состава компонентов программы.

Шаг 2. Параметры задачи изменения компонентов программы

Выберите компоненты программы, которые будут доступны на компьютере пользователя.

Установите флажок Удалять несовместимые программы сторонних производителей. Список несовместимых программ можно просмотреть в `incompatible.txt`, который входит в комплект поставки. Если на компьютере установлены несовместимые программы, установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready завершается с ошибкой.

Если требуется, включите защиту паролем на выполнение задачи:

1. Нажмите на кнопку Дополнительно.
2. Установите флажок Использовать пароль для изменения состава компонентов.
3. Введите учетные данные пользователя KLAdmin.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 5. Определение названия задачи

Введите название задачи, например, Добавление компонента Контроль программ.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок Запустить задачу после завершения работы мастера. Вы можете следить за ходом выполнения задачи в свойствах задачи.

В результате на компьютерах пользователей будет изменен состав компонентов Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в тихом режиме. В локальном интерфейсе программы будут отображаться параметры доступных компонентов. Компоненты, которые не вошли в состав программы, выключены, а параметры этих компонентов недоступны.

Как добавить или удалить компоненты программы в Web Console и Cloud Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Добавить.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке Программа выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).

2. В раскрывающемся списке Тип задачи выберите Изменение состава компонентов программы.

3. В поле Название задачи введите короткое описание, например, `Добавление компонента Контроль программ`.

4. В блоке Выбор устройств, которым будет назначена задача выберите область действия задачи.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Например, выберите отдельную группу администрирования или сделайте выборку.

Шаг 3. Завершение создание задачи

Установите флажок Открыть окно свойств задачи после ее создания и завершите работу мастера. В свойствах задачи выберите закладку Параметры программы и выберите компоненты программы, которые будут доступны.

Если требуется, включите защиту паролем на выполнение задачи:

1. В блоке Дополнительные параметры установите флажок Использовать пароль для изменения состава компонентов.

2. Введите учетные данные пользователя KLAdmin.

Сохраните внесенные изменения и запустите задачу.

В результате на компьютерах пользователей будет изменен состав компонентов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в тихом режиме. В локальном интерфейсе программы будут отображаться параметры доступных компонентов. Компоненты, которые не вошли в состав программы, выключены, а параметры этих компонентов недоступны.

Обновление предыдущей версии программы

Обновление предыдущей версии программы имеет следующие особенности:

- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11.4.0 совместим с Kaspersky Security Center версии 12.
- Перед началом обновления программы рекомендуется закрыть все работающие программы.
- Если на компьютере установлены жесткие диски, к которым применено полнодисковое шифрование (FDE), для обновления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с версии 10 до версии 11.0.0 и более поздней нужно расшифровать все зашифрованные жесткие диски.

Перед обновлением Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует функциональность полнодискового шифрования. Если функциональность полнодискового шифрования не удалось заблокировать, установка обновления не начнется. После обновления программы функциональность полнодискового шифрования будет восстановлена.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает обновление следующих версий программы:

- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 1 Maintenance Release 4 для Windows (сборка 10.2.6.3733).
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 Maintenance Release 1 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 Maintenance Release 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 Maintenance
- Release 3 для Windows (сборка 10.3.3.275). Kaspersky Endpoint Security для бизнеса - Расширенный
- EDR Ready 10 Service Pack 2 Maintenance Release 4 для Windows (сборка 10.3.3.275).
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.0.0 (сборка 11.0.0.6499).
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.0.1 (сборка 11.0.1.90).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.1.0 (сборка 11.1.0.15919).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.1.1 (сборка 11.1.1.126).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.2.0 (сборка 11.2.0.2254).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows 11.3.0 (сборка 11.3.0.773).

При обновлении Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows до Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows

11.4.0 в резервное хранилище новой версии программы переносятся файлы, помещенные в резервное хранилище и на карантин в предыдущей версии программы. Для более ранних версий Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, чем Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows, перенос файлов, помещенных в резервное хранилище и на карантин в предыдущей версии программы, не осуществляется.

Программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может быть обновлена на компьютере следующими способами:

- локально с помощью мастера установки программы.
- локально из командной строки. удаленно с
- помощью Kaspersky Security Center 12. •

удаленно через редактор управления групповыми

политиками Microsoft Windows (подробнее см. на

сайте Службы технической поддержки

Microsoft).

- удаленно с помощью System Center Con guration Manager.

Если в сети организации развернута программа с набором компонентов, отличным от набора по умолчанию, обновление программы через Консоль администрирования (MMC) отличается от обновления программы через Web Console и Cloud Console. Обновление Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready имеет следующие особенности:

- Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

  Если вы создали инсталляционный пакет новой версии программы с набором компонентов по умолчанию, после обновления набор компонентов на компьютере пользователя не будет изменен. Для использования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с набором компонентов по умолчанию нужно открыть свойства инсталляционного пакета, изменить набор компонентов, вернуть набор компонентов в исходное состояние и сохранить изменения.

- Консоль администрирования (MMC) Kaspersky Security Center.

  Набор компонентов программы после обновления будет соответствовать набору компонентов в инсталляционном пакете. То есть если новая версия программы имеет набор компонентов по умолчанию, то, например, компонент Защита от атак BadUSB будет удален с компьютера, так как этот компонент исключен из набора по умолчанию. Для продолжения использования программы с прежним набором компонентов нужно выбрать необходимые компоненты в параметрах инсталляционного пакета.

Удаление программы

В результате удаления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready компьютер и данные пользователя окажутся незащищенными.

Программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready может быть удалена с

- компьютера следующими способами: локально с помощью мастера установки программы;
- локально из командной строки; удаленно с помощью Kaspersky Security Center (подробнее см. в
- справке Kaspersky Security Center);
- удаленно через редактор управления групповыми политиками Microsoft Windows (подробнее см. на сайте Службы технической поддержки Microsoft).

Удаление через Kaspersky Security Center

Вы можете удалить программу дистанционно с помощью задачи Удаленная деинсталляция программы. При выполнении задачи Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready загрузит на компьютер пользователя утилиту для удаления программы. После завершения удаления программы, утилита будет удалена автоматически.

Как удалить программу через Консоль администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Новая задача.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите Сервер администрирования Kaspersky Security Center → Дополнительно → Удаленная деинсталляция программы.

Шаг 2. Выбор удаляемой программы

Выберите Удалить программу, поддерживаемую Kaspersky Security Center.

Шаг 3. Параметры задачи удаления программы

Выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).

Шаг 4. Параметры утилиты деинсталляции

Настройте следующие дополнительные параметры программы:

- Принудительно загрузить утилиту деинсталляции. Выберите средства доставки утилиты:

- С помощью Агента администрирования. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляется средствами Агента администрирования.

- Средствами Microsoft Windows с помощью Сервера администрирования. Доставка утилиты на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

- Средствами операционной системы с помощью точек распределения. Утилита передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точках распространения см. в справке Kaspersky Security Center.

- Предварительно проверять версию операционной системы. Если требуется, снимите этот флажок. Это позволит избежать загрузки утилиты деинсталляции, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютеров соответствует программным требованиям, проверку можно пропустить.

Если операция удаления программы защищена паролем, выполните следующие действия:

1. Установите флажок Использовать пароль деинсталляции.

2. Нажмите на кнопку Изменить.

3. Введите пароль учетной записи KLAdmin.

Шаг 5. Выбор параметра перезагрузки операционной системы

После удаления программы требуется перезагрузка. Выберите действие, которое будет выполняться для перезагрузки компьютера.

Шаг 6. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 7. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для удаления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 8. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 9. Определение названия задачи

Введите название задачи, например, `Удаление Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11.4.0`.

Шаг 10. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок Запустить задачу после завершения работы мастера. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Удаление программы будет выполнено в тихом режиме.

Как удалить программу через Web Console и Cloud Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Добавить.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающимся списке Программа выберите Kaspersky Security Center.
2. В раскрывающемся списке Тип задачи выберите Удаленная деинсталляция программы.
3. В поле Название задачи введите короткое описание, например, `Удаление Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на компьютерах Службы технической поддержки`.
4. В блоке Выбор устройств, которым будет назначена задача выберите область действия задачи.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Например, выберите отдельную группу администрирования или сделайте выборку.

Шаг 3. Настройка параметров удаления программы

На этом шаге настройте параметры удаления программы:

1. Выберите тип Удалить управляемую программу.
2. Выберите программу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).
3. Принудительно загрузить утилиту деинсталляции. Выберите средства доставки утилиты:

   - С помощью Агента администрирования. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляется средствами Агента администрирования.
   - Средствами Microsoft Windows с помощью Сервера администрирования. Доставка утилиты на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

- Средствами операционной системы с помощью точек распределения. Утилита передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точках распространения см. в справке Kaspersky Security Center.

4. В поле Максимальное количество одновременных загрузок установите ограничение количества запросов к Серверу администрирования для загрузки утилиты для удаления программы. Ограничение запросов позволит избежать перегрузки сети.

5. В поле Количество попыток деинсталляции установите ограничение попыток удалить программу. Если удаление Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready завершается с ошибкой, задача автоматически запускает удаление повторно.

6. Если требуется, снимите флажок Предварительно проверять версию операционной системы. Это позволит избежать загрузки утилиты деинсталляции, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютеров соответствует программным требованиям, проверку можно пропустить.

Шаг 4. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для удаления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 5. Завершение создания задачи

Завершите работу мастера по кнопке Готово. В списке задач отобразится новая задача.

Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку Запустить. Удаление программы будет выполнено в тихом режиме. После завершения удаления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready покажет запрос на перезагрузку компьютера.

> Если операция удаления программы защищена паролем, введите пароль учетной записи KLAdmin в свойствах задачи Удаленная деинсталляция программы. Без пароля задача не будет выполнена.

Чтобы использовать пароль учетной записи KLAdmin в задаче Удаленная деинсталляция программы, выполните следующие действия:

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Security Center Удаленная деинсталляция программы.

   Откроется окно свойств задачи.

3. Выберите закладку Параметры программы.

4. Установите флажок Использовать пароль деинсталляции.

5. Введите пароль учетной записи KLAdmin.

6. Нажмите на кнопку Сохранить.

Удаление программы с помощью мастера

Удаление Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняется обычным способом, принятым для операционной системы Windows, через Панель управления. Запустится мастер установки программы. Следуйте указаниям на экране.

Вы можете указать, какие используемые программой данные вы хотите сохранить для дальнейшего использования при повторной установке программы (например, ее более новой версии). Если вы не укажете никаких данных, программа будет удалена полностью.

Вы можете сохранить следующие данные:

- Информация об активации – данные, позволяющие в дальнейшем не активировать программу повторно. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически добавляет лицензионный ключ, если срок действия лицензии не истек к моменту установки.

- Файлы резервного хранилища – файлы, проверенные программой и помещенные в резервное хранилище.

  Доступ к файлам резервного хранилища, сохраненным после удаления программы, возможен только из той же версии программы, в которой они были сохранены.

  Если вы планируете использовать объекты резервного хранилища после удаления программы, вам нужно восстановить их до удаления программы. Однако эксперты "Лаборатории Касперского" не рекомендуют восстанавливать объекты из резервного хранилища, так как это может нанести вред компьютеру.

- Параметры работы программы – значения параметров работы программы, установленные в процессе ее настройки.

- Локальное хранилище ключей шифрования – данные, которые обеспечивают доступ к зашифрованным до удаления программы файлам и дискам. Для доступа к зашифрованным файлам и дискам убедитесь, что вы выбрали функциональность шифрования данных при повторной установке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Дополнительных действий для доступа к зашифрованным раннее файлам и дискам выполнять не требуется.

Удаление программы из командной строки

Удаление Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки программы.

- В тихом режиме. После запуска удаления в тихом режиме ваше участие в процессе удаления не требуется. Для удаления программы в тихом режиме используйте ключи `/s` и `/qn`.

Чтобы удалить программу в тихом режиме, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.

2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

3. Выполните команду:

- Если операция удаления не защищена паролем:

  `setup_kes.exe /s /x` **или**

  `msiexec.exe /x <GUID> /qn`

  где `<GUID>` **– уникальный идентификатор программы. Вы можете узнать GUID программы с помощью команды:**

  ```
  wmic product where "Name like '%Kaspersky Endpoint Security для бизнеса -  Расширенный EDR Ready%'" get Name, IdentifyingNumber
  ```

- Если операция удаления защищена паролем:

  `setup_kes.exe /pKLLOGIN=<имя пользователя> /pKLPASSWD=<пароль> /s /x`

  или `msiexec.exe /x <GUID> KLLOGIN=<имя пользователя> KLPASSWD=<пароль> /qn`

  Пример:
  ```
  msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=!Password1 /qn
  ```

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Рекомендуется внимательно ознакомиться с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в интерактивном режиме.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы, а также находится в папке установки программы `%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready for Windows\Doc\<локаль>\KES`.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- Пробная – бесплатная лицензия, предназначенная для ознакомления с программой.

  Пробная лицензия обычно имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать программу по пробной лицензии только один раз.

- Коммерческая – платная лицензия, предоставляемая при приобретении программы.

  Функциональность программы, доступная по коммерческой лицензии, зависит от выбора продукта. Выбранный продукт указан в Лицензионном сертификате. Информацию о доступных продуктах вы можете найти на сайте "Лаборатории Касперского".

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью. Вы можете использовать компоненты защиты и контроля и выполнять проверку на основе баз программы, установленных до истечения срока действия лицензии. Кроме того, программа продолжает шифровать изменяющиеся файлы, зашифрованные до истечения срока действия лицензии, но не шифрует новые файлы. Использование Kaspersky Security Network недоступно.

  Чтобы продолжить использование Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой

- лицензии: лицензионный ключ или номер заказа; информация о пользователе, которому
- предоставляется лицензия; информация о программе, которую можно активировать по
- предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых

можно использовать программу по предоставляемой лицензии); дата начала срока действия

- лицензии; дата окончания срока действия лицензии или срок действия лицензии; тип
- лицензии.
-

О подписке

Подписка на Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме или отказаться от нее. Управление подпиской доступно на веб-сайте поставщика услуг.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready после истечения ограниченной подписки вам нужно ее продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность программы сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready по подписке, вам нужно применить код активации, предоставленный поставщиком услуг. После применения кода активации добавляется активный ключ, определяющий лицензию на использование программы по подписке. Добавить резервный ключ по подписке невозможно.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения.

Для ключа, добавленного по подписке, Лицензионный сертификат не предоставляется.

Вы можете добавить лицензионный ключ в программу одним из следующих способов: применить файл ключа или ввести код активации.

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для обеспечения работы программы вам нужно добавить другой ключ.

Ключ может быть активным и резервным.

Активный ключ – ключ, используемый в текущий момент для работы программы. В качестве активного ключа может быть добавлен ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного ключа.

Резервный ключ – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. По истечении срока годности активного ключа резервный ключ автоматически становится активным. Резервный ключ может быть добавлен только при наличии активного ключа.

Ключ для пробной лицензии может быть добавлен только в качестве активного ключа. Он не может быть добавлен в качестве резервного ключа. Ключ для пробной лицензии не может заменить активный ключ для коммерческой лицензии.

Если ключ попадает в черный список ключей, в течение восьми дней доступна функциональность программы, определенная лицензией, по которой программа активирована. Программа уведомляет пользователя о том, что ключ помещен в черный список ключей. По истечении восьми дней функциональность программы соответствует ситуации, когда истекает срок действия лицензии. Вы можете использовать компоненты защиты и контроля и выполнять проверку на основе баз программы, установленных до истечения срока действия лицензии. Кроме того, программа продолжает шифровать изменяющиеся файлы, зашифрованные до истечения срока действия лицензии, но не шифрует новые файлы. Использование Kaspersky Security Network недоступно.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

При активации программы с помощью кода активации добавляется активный ключ. При этом резервный ключ может быть добавлен только с помощью кода активации и не может быть добавлен с помощью файла ключа.

Если код активации был потерян после активации программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского".

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready или после заказа пробной версии Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.

При активации программы с помощью файла ключа добавляется активный ключ. При этом резервный ключ может быть добавлен только с помощью файла ключа и не может быть добавлен с помощью кода активации.

Активация программы

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии. Активация программы заключается в добавлении лицензионного ключа.

Вы можете активировать программу одним из следующих способов:

- Локально из интерфейса программы с помощью мастера активации программы. Этим способом вы можете добавить и активный, и резервный ключ.

- Удаленно с помощью программного комплекса Kaspersky Security Center путем создания и последующего запуска задачи добавления лицензионного ключа. Этим способом вы можете добавить и активный, и резервный ключ.

- Удаленно путем распространения на клиентские компьютеры файлов ключей и кодов активации, размещенных в хранилище ключей на Сервере администрирования Kaspersky Security Center. Подробнее о распространении ключей см. в справке Kaspersky Security Center. Этим способом вы можете добавить и активный, и резервный ключ.

  Код активации, приобретенный по подписке, распространяется в первую очередь.

- С помощью командной строки.

Во время активации программы, удаленно или во время установки программы в тихом режиме, с помощью кода активации возможна произвольная задержка, связанная с распределением нагрузки на серверы активации "Лаборатории Касперского". Если требуется немедленная активация программы, вы можете прервать выполняющуюся активацию и запустить активацию программы с помощью мастера активации программы.

Активация программы через Kaspersky Security Center

Вы можете активировать программу дистанционно через Kaspersky Security Center следующими способами:

- С помощью задачи Добавить ключ.

  Этот способ позволяет добавить ключ на конкретный компьютер или компьютеры, входящие в группу администрирования.

- Путем распространения на компьютеры ключа, размещенного на Сервере администрирования Kaspersky Security Center.

  Этот способ позволяет автоматически добавлять ключ на компьютеры, уже подключенные к Kaspersky Security Center, а также на новые компьютеры. Для использования этого способа вам нужно сначала добавить ключ на Сервер администрирования Kaspersky Security Center. Подробнее о добавлении ключей на Сервер администрирования Kaspersky Security Center см. в справке Kaspersky Security Center.

Для Kaspersky Security Center Cloud Console предусмотрена пробная версия. Пробная версия – это специальная версия Kaspersky Security Center Cloud Console, предназначенная для ознакомления пользователя с функциями Kaspersky Security Center Cloud Console. В этой версии вы можете выполнять действия в рабочем пространстве в течении 30 дней. Все управляемые программы запускаются по пробной лицензии Kaspersky Security Center Cloud Console автоматически, включая Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. При этом активировать Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready по собственной пробной лицензии по истечении пробной лицензии Kaspersky Security Center Cloud Console невозможно. Подробнее о лицензировании Kaspersky Security Center см. в справке Kaspersky Security Center Cloud Console.

Пробная версия Kaspersky Security Center Cloud Console не позволяет вам впоследствии перейти на коммерческую версию. Любое пробное рабочее пространство будет автоматически удалено со всем его содержимым по истечении 30-дневного срока.

Вы можете контролировать использование лицензий следующими способами:

- Просмотреть Отчет об использовании ключей в инфраструктуре организации (Мониторинг и отчеты → Отчеты).
- Просмотреть статусы компьютеров на закладке Устройства → Управляемые устройства. Если программа не активирована, то у компьютера будет статус ⚠ и описание статуса Программа не активирована.
- Просмотреть информацию о лицензии в свойствах компьютера.
- Просмотреть свойства ключа (Операции → Лицензирование). Как

активировать программу в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Новая задача.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0) → Добавление ключа.

Шаг 2. Добавление ключа

Введите код активации или выберите файл ключа.

Подробнее о добавлении ключей в хранилище Kaspersky Security Center см. в справке Kaspersky Security Center.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 5. Определение названия задачи

Введите название задачи, например, `Активация Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows`.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок Запустить задачу после завершения работы мастера. Вы можете следить за ходом выполнения задачи в свойствах задачи. В результате на компьютерах пользователей будет активирована программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в тихом режиме (статус лицензии).

Как активировать программу в Web Console и Cloud Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Добавить.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке Программа выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).

2. В раскрывающемся списке Тип задачи выберите Добавление ключа.

3. В поле Название задачи введите короткое описание, например, `Активация Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows`.

4. В блоке Выбор устройств, которым будет назначена задача выберите область действия задачи. Нажмите на кнопку Далее.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.

- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Выбор лицензии

Выберите лицензию, по которой вы хотите активировать программу. Нажмите на кнопку Далее.

Вы можете добавлять ключи в Web Console (Операции → Лицензирование).

Шаг 4. Завершение создания задачи

Завершите работу мастера по кнопке Готово. В списке задач отобразится новая задача. Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку Запустить. В результате на

компьютерах пользователей будет активирована программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в тихом режиме (статус лицензии).

В свойствах задачи Добавить ключ вы можете добавить на компьютер резервный ключ. Резервный ключ становится активным либо по истечении срока годности активного ключа, либо при удалении активного ключа. Наличие резервного ключа позволяет избежать ограничения функциональности программы в момент окончания срока действия лицензии.

Как автоматически добавить лицензионный ключ на компьютеры через Консоль администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Лицензии Лаборатории Касперского.

Откроется список лицензионных ключей.

2. Откройте свойства лицензионного ключа.

3. В разделе Общие установите флажок Автоматически распространяемый лицензионный ключ.

4. Сохраните внесенные изменения.

В результате ключ будет автоматически распространяться на компьютеры, для которых он подходит. При автоматическом распространении ключа в качестве активного или резервного учитывается лицензионное ограничение на количество компьютеров, заданное в свойствах ключа. Если лицензионное ограничение достигнуто, распространение ключа на компьютеры автоматически прекращается. Вы можете просмотреть количество компьютеров, на которые добавлен ключ, и другие данные в свойствах ключа в разделе Устройства.

Как автоматически добавить лицензионный ключ на компьютеры через Web Console и Cloud Console

1. В главном окне Web Console выберите Операции → Лицензирование → Лицензии "Лаборатории Касперского".

Откроется список лицензионных ключей.

2. Откройте свойства лицензионного ключа.

3. На закладке Общие включите переключатель Распространять ключ автоматически.

4. Сохраните внесенные изменения.

В результате ключ будет автоматически распространяться на компьютеры, для которых он подходит. При автоматическом распространении ключа в качестве активного или резервного учитывается лицензионное ограничение на количество компьютеров, заданное в свойствах ключа. Если лицензионное ограничение достигнуто, распространение ключа на компьютеры автоматически прекращается. Вы можете просмотреть количество компьютеров, на которые добавлен ключ, и другие данные в свойствах ключа на закладке Устройства.

Активация программы с помощью мастера активации программы

Чтобы активировать Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с помощью мастера активации программы, выполните следующие действия:

1. Нажмите на кнопку / , расположенную в нижней части главного окна программы.
2. В открывшемся окне нажмите на кнопку Активировать программу по коммерческой лицензии.

Запустится мастер активации программы. Следуйте указаниям мастера активации программы.

Активация программы с помощью командной строки

Чтобы активировать программу с помощью командной строки,

введите в командной строке:

```
avp.com license /add <код активации или файл ключа> [/login=<имя пользователя> /password=<пароль>]
```

Учетные данные пользователя (`/login=<имя пользователя> /password=<пароль>`) нужно ввести, если включена Защита паролем.

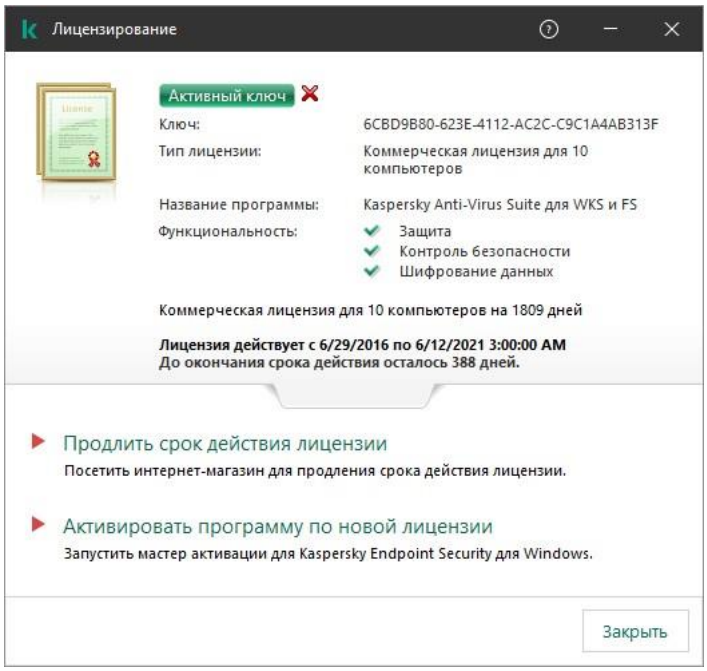
Просмотр информации о лицензии

Чтобы просмотреть информацию о лицензии, внизу

главного окна программы нажмите на значок /

.

Откроется окно Лицензирование, в котором представлена информация о лицензии (см. рис. ниже).



Окно Лицензирование

В окне Лицензирование представлена следующая информация:

- Статус ключа. На компьютере может быть несколько ключей. Ключ может быть активным и резервным. В программе не может быть больше одного активного ключа. Резервный ключ может стать активным только после истечения срока годности активного ключа или после удаления активного ключа по кнопке ×.
- Ключ. Ключ – это уникальная буквенно-цифровая последовательность, которая формируется из кода активации или файла ключа.
- Тип лицензии. Предусмотрены следующие типы лицензий: пробная и коммерческая.
- Название программы. Полное название приобретенной программы "Лаборатории Касперского".
- Функциональность. Функции программы, которые доступны по вашей лицензии. Предусмотрены следующие функции: Защита, Контроль безопасности, Шифрование данных и другие. Список доступных функций также указан в Лицензионном сертификате.
- Дополнительная информация о лицензии. Тип лицензии, количество компьютеров, на которые распространяется лицензия, дата начала и дата и время окончания срока действия лицензии (только для активного ключа).

> Время окончания срока действия лицензии отображается в часовом поясе, настроенном в операционной системе.

Также в окне лицензирования доступны следующие действия:

- Приобрести лицензию / Продлить срок действия лицензии. Открывает веб-сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию или продлить срок действия лицензии. Для этого вам будет нужно ввести данные организации и оплатить заказ.

- Активировать программу по новой лицензии. Запускает мастер активации программы. Мастер позволяет добавить ключ с помощью кода активации или файла ключа. Мастер активации программы позволяет добавить активный ключ и только один резервный ключ.

Приобретение лицензии

Вы можете приобрести лицензию уже после установки программы. Приобретя лицензию, вы получите код активации или файл ключа, с помощью которых нужно активировать программу.

Чтобы приобрести лицензию, выполните следующие действия:

1. В главном окне программы нажмите на кнопку / .

   Откроется окно Лицензирование.

2. В окне Лицензирование выполните одно из следующих действий:

   - Нажмите на кнопку Приобрести лицензию, если не добавлен ни один ключ или добавлен ключ для пробной лицензии.

   - Нажмите на кнопку Продлить срок действия лицензии, если добавлен ключ для коммерческой лицензии.

   Откроется веб-сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию.

Продление подписки

При использовании программы по подписке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки.

Если вы используете программу по неограниченной подписке, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически в фоновом режиме проверяет наличие обновленного ключа на сервере активации. Если на сервере активации есть ключ, программа добавляет его в режиме замены предыдущего ключа. Таким образом неограниченная подписка на Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready продлевается без вашего участия.

Если вы используете программу по ограниченной подписке, в день истечения подписки или льготного периода после истечения подписки, во время которого доступно ее продление, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready уведомляет вас об этом и прекращает попытки автоматического продления подписки. Поведение Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready при этом соответствует ситуации, когда истекает срок действия коммерческой лицензии на использование программы, – программа работает без обновлений и Kaspersky Security Network недоступен.

Вы можете продлить подписку на веб-сайте поставщика услуг.

Вы можете обновить статус подписки вручную в окне Лицензирование. Это может потребоваться, если подписка продлена после истечения льготного периода, и программа автоматически не обновляет статус подписки.

Чтобы перейти на веб сайт поставщика услуг из интерфейса программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку / .

   Откроется окно Лицензирование.

2. В окне Лицензирование нажмите на кнопку Связаться с поставщиком подписки.

Предоставление данных

Если для активации Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready применяется код активации, с целью проверки правомерности использования программы вы соглашаетесь

- периодически передавать в автоматическом режиме в "Лабораторию Касперского" следующую информацию: тип, версию и локализацию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready; версии установленных обновлений Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready; идентификатор компьютера и идентификатор установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на компьютере; серийный номер и идентификатор активного ключа;

тип, версию и разрядность операционной системы, название виртуальной среды, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена в виртуальной среде;

- идентификаторы компонентов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, активных на момент предоставления информации.

"Лаборатория Касперского" может также использовать эту информацию для формирования статистической информации о распространении и использовании программного обеспечения "Лаборатории Касперского".

Используя код активации, вы соглашаетесь на автоматическую передачу данных, перечисленных выше. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", для активации Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready следует использовать файл ключа.

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в автоматическом режиме следующую информацию:

- При обновлении Kaspersky Endpoint Security для бизнеса –
  - Расширенный EDR Ready: версию Kaspersky Endpoint Security
  - для бизнеса – Расширенный EDR Ready; идентификатор
  - Kaspersky Endpoint Security для бизнеса – Расширенный EDR
  - Ready; активный ключ; уникальный идентификатор запуска
  - задачи обновления; уникальный идентификатор установки
- Kaspersky Endpoint Security для бизнеса – Расширенный EDR
  - Ready.
  - При переходе по ссылкам из интерфейса Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready:
  - версию Kaspersky Endpoint Security для
  - бизнеса – Расширенный EDR Ready;
  - версию операционной системы; дату
  - активации Kaspersky Endpoint Security для
  - бизнеса – Расширенный EDR Ready; дату
  - окончания действия лицензии; дату создания
  - ключа; дату установки Kaspersky Endpoint
  - Security для бизнеса – Расширенный EDR
  - Ready; идентификатор Kaspersky Endpoint
  - Security для бизнеса – Расширенный EDR
  - Ready; идентификатор обнаруженной
  - уязвимости операционной системы;
  - идентификатор последнего установленного
  - обновления для Kaspersky Endpoint Security
  - для бизнеса – Расширенный EDR Ready;
  - хеш обнаруженного файла, представляющего угрозу, и название этого объекта по классификации

"Лаборатории Касперского"; категорию ошибки активации Kaspersky Endpoint

- Security для бизнеса - Расширенный EDR Ready; код ошибки активации
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready;
- количество дней до истечения срока годности ключа; количество дней,
- прошедших с момента добавления ключа; количество дней, прошедших с
- момента окончания срока действия лицензии; количество компьютеров, на
- которые распространяется действующая лицензия; активный ключ; срок
- действия лицензии Kaspersky Endpoint Security для бизнеса - Расширенный
- EDR Ready; текущий статус лицензии; тип действующей лицензии; тип
- программы; уникальный идентификатор запуска задачи обновления;
- уникальный идентификатор установки Kaspersky Endpoint Security для бизнеса
- - Расширенный EDR Ready на компьютере; язык интерфейса Kaspersky
- Endpoint Security для бизнеса - Расширенный EDR Ready.
- Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского".
- Данные передаются по зашифрованным каналам связи.

Более подробную информацию о получении, обработке, хранении и уничтожении информации об использовании программы после принятия Лицензионного соглашения и согласия с Положением о Kaspersky Security Network вы можете узнать, прочитав тексты этих документов, а также на веб-сайте "Лаборатории Касперского". Файлы license.txt и ksn_<ID языка>.txt с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки программы.

Начало работы

После установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready вы можете управлять программой с помощью следующих интерфейсов:

- Локальный интерфейс программы.
- Консоль администрирования Kaspersky Security Center.
- Kaspersky Security Center 12 Web Console.
- Kaspersky Security Center Cloud Console.

Консоль администрирования Kaspersky Security Center

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, настраивать параметры работы

программы, изменять состав компонентов программы, добавлять ключи, запускать и останавливать задачи обновления и проверки.

Управление программой через Kaspersky Security Center осуществляется с помощью плагина управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Подробнее об управлении программой через Kaspersky Security Center см. в справке Kaspersky Security Center.

Kaspersky Security Center 12 Web Console и Cloud Console

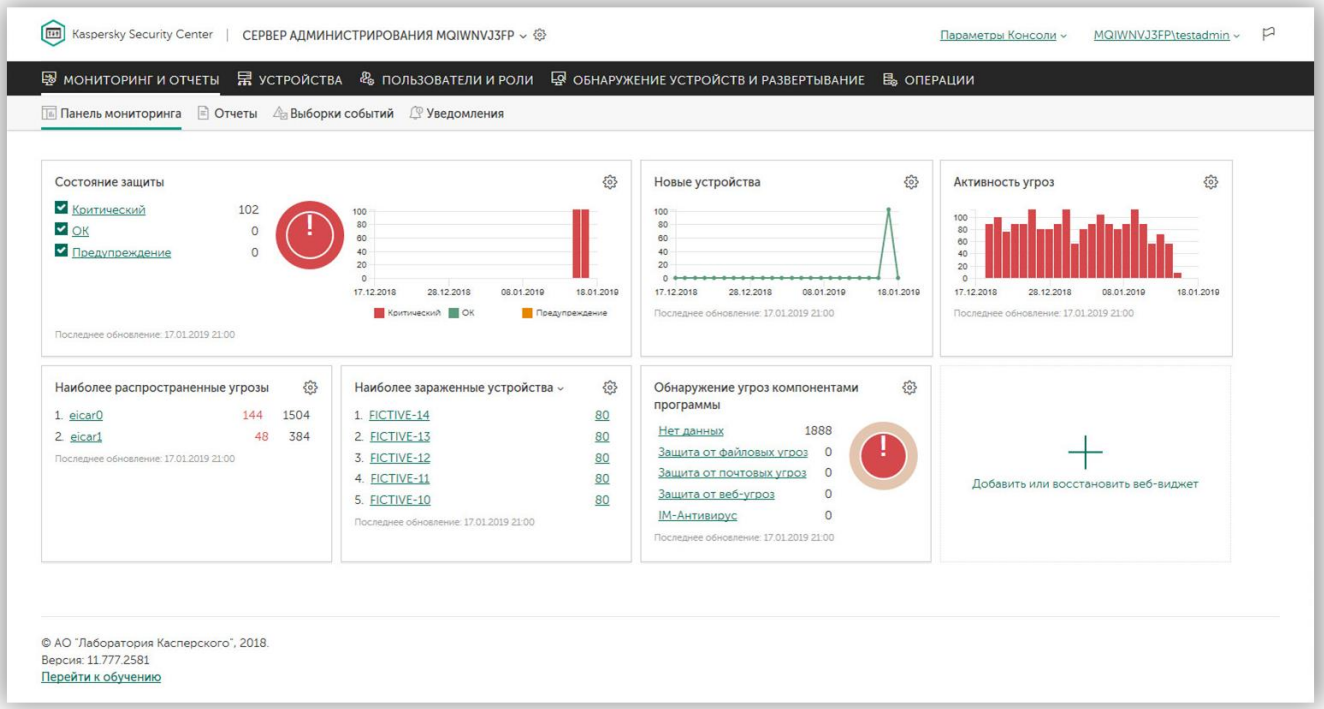
Kaspersky Security Center 12 Web Console (далее также "Web Console") представляет собой программу (вебприложение), предназначенную для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Web Console является компонентом Kaspersky Security Center, предоставляющим пользовательский интерфейс. Подробную информацию о Kaspersky Security Center 12 Web Console см. в справке Kaspersky Security Center.

Kaspersky Security Center Cloud Console (далее также "Cloud Console") представляет собой облачное решение для защиты и контроля сети организации. Подробную информацию о Kaspersky Security Center Cloud Console см. в справке Kaspersky Security Center Cloud Console.

С помощью Web Console и Cloud Console вы можете выполнять следующие

- действия: контролировать состояние системы безопасности вашей
- организации; устанавливать программы "Лаборатории Касперского" на
- устройства вашей сети; управлять установленными программами;
- просматривать отчеты о состоянии системы безопасности.

Управление программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через Web Console, Cloud Console и Консоль администрирования Kaspersky Security Center отличается. Также отличается список доступных компонентов и задач.



Интерфейс Kaspersky Security Center 12 Web Console

О плагине управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows

Плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows обеспечивает взаимодействие Kaspersky
Endpoint Security с Kaspersky Security Center. Плагин управления позволяет управлять Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с помощью следующих инструментов: политики, задачи, а также локальные параметры программы. Для взаимодействия с Kaspersky Security Center 12 Web Console предназначен веб-плагин.

Версия плагина управления может отличаться от версии программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, установленной на клиентском компьютере. Если в установленной версии плагина управления предусмотрено меньше функций, чем в установленной версии Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, то параметры недостающих функций не регулируются плагином управления. Такие параметры могут быть изменены пользователем в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Веб-плагин по умолчанию не установлен в Kaspersky Security Center 12 Web Console. В отличие от плагина управления для Консоли администрирования Kaspersky Security Center, который устанавливается на рабочее место администратора, веб-плагин требуется установить на компьютер с установленной программой Kaspersky Security Center 12 Web Console. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Web Console в браузере. Вы можете просмотреть список установленных вебплагинов в интерфейсе Web Console (Параметры Консоли → Плагины). Подробнее о совместимости версий веб-плагинов и Web Console см. в справке Kaspersky Security Center.

Установка веб-плагина

Вы можете установить веб-плагин следующими способами:

- Установить веб-плагин с помощью мастера первоначальной настройки Kaspersky Security Center 12 Web Console.

  Web Console автоматически предлагает запустить мастер первоначальной настройки при первом подключении Web Console к Серверу администрирования. Также вы можете запустить мастер первоначальной настройки в интерфейсе Web Console (Обнаружение устройств и развертывание → Развертывание и назначение → Мастер первоначальной настройки). Мастер первоначальной настройки также может проверить актуальность установленных веб-плагинов и загрузит необходимые обновления для них. Подробнее о мастере первоначальной настройки Kaspersky Security Center 12 Web Console см. в справке Kaspersky Security Center.

- Установить веб-плагин из списка доступных дистрибутивов в Web Console.

  Для установки веб-плагина требуется выбрать дистрибутив веб-плагина Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в интерфейсе Web Console (Параметры Консоли → Плагины). Список доступных дистрибутивов обновляется автоматически после выпуска новых версий программ "Лаборатории Касперского".

- Загрузить дистрибутив в Web Console из стороннего источника.

  Для установки веб-плагина требуется добавить ZIP-архив дистрибутива веб-плагина Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в интерфейсе Web Console (Параметры Консоли → Плагины). Дистрибутив веб-плагина вы можете загрузить, например, на веб-сайте "Лаборатории Касперского".

Обновление плагина управления

Для обновления плагина управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows требуется загрузить последнюю версию плагина управления (входит в комплект поставки) и запустить мастер установки плагина.

При появлении новой версии веб-плагина Web Console отобразит уведомление Доступны обновления для используемых плагинов. Вы можете перейти к обновлению версии веб-плагина из уведомления Web Console.
Также вы можете проверить наличие обновлений веб-плагина вручную в интерфейсе Web Console (Параметры Консоли → Плагины). Предыдущая версия веб-плагина будут автоматически удалена во время обновления.

> При обновлении веб-плагина сохраняются уже существующие элементы (например, политики или задачи). Новые параметры элементов, реализующие новые функции Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, появятся в существующих элементах и будут иметь значения по умолчанию.

Вы можете обновить веб-плагин следующими способами:

- Обновить веб-плагин в списке веб-плагинов в онлайн-режиме.

  Для обновления веб-плагина требуется выбрать дистрибутив веб-плагина Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в интерфейсе Web Console и запустить обновление

(Параметры Консоли → Плагины). Web Console проверит наличие обновлений на серверах "Лаборатории Касперского" и загрузит необходимые обновления.

- Обновить веб-плагин из файла.

  Для обновления веб-плагина требуется выбрать ZIP-архив дистрибутива веб-плагина Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в интерфейсе Web Console (Параметры Консоли → Плагины). Дистрибутив веб-плагина вы можете загрузить, например, на веб-сайте "Лаборатории Касперского". Вы можете обновить веб-плагин Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready только до более новой версии. Обновить веб-плагин до более старой версии невозможно.

При открытии любого элемента (например, политики или задачи) веб-плагин проверяет информацию о совместимости. Если версия веб-плагина равна или выше версии, указанной в информации о совместимости, то вы можете изменять параметры этого элемента. В противном случае изменение параметров выбранного элемента с помощью веб-плагина недоступно. Рекомендуется обновить веб-плагин.

Особенности работы с плагинами управления разных версий

Для управления программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через Kaspersky Security Center требуется плагин управления, версия которого равна или выше версии, указанной в информации о совместимости Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с плагином управления. Вы можете посмотреть минимальную необходимую версию плагина управления в файле installer.ini, входящем в комплект поставки.

При открытии любого элемента (например, политики или задачи) плагин управления проверяет информацию о совместимости. Если версия плагина управления равна или выше версии, указанной в информации о совместимости, то вы можете изменять параметры этого элемента. В противном случае изменение параметров выбранного элемента с помощью плагина управления недоступно. Рекомендуется обновить плагин управления.

Обновление плагина управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 для Windows

Если в Консоли администрирования установлен плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 для Windows, то установка плагина управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows имеет следующие особенности:

- Плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 для Windows не будет удален и останется доступным для работы.
- Плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows не поддерживает управление программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 для Windows на компьютерах пользователей.
- Плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows не поддерживает элементы (например, политики или задачи), созданные с помощью плагина управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 для Windows.

Если вы удалили плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 для Windows и установили плагин управления Kaspersky Endpoint Security для бизнеса -

Расширенный EDR Ready 11 для Windows, вам нужно создать новые политики, задачи и т.п. Также вы можете установить плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows с плагином управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 для Windows для выполнения миграции. После выполнения миграции удалите плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 для Windows.

Обновление плагина управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows

Если в Консоли администрирования установлен плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows, то установка новой версии плагина управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows имеет следующие особенности:

- Предыдущая версия плагина управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows будет удалена.
- Плагин управления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows новой версии поддерживает управление программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11 для Windows предыдущей версии на компьютерах пользователей.
- С помощью плагина управления новой версии вы можете изменять параметры в политиках, задачах и т.п., созданных плагином управления предыдущей версии.

- Для новых параметров плагин управления новой версии устанавливает значения по умолчанию при первом сохранении политики, профиля политики или задачи.

  После обновления плагина управления рекомендуется проверить и сохранить значения новых параметров в политиках и профилях политик. Если вы этого не сделаете, новые блоки параметров Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready на компьютере пользователя будут иметь значения по умолчанию и доступны для изменения (атрибут). Рекомендуется выполнять проверку начиная с политик и профилей политик верхнего уровня иерархии. Также рекомендуется использовать учетную запись пользователя, для которой настроены права доступа ко всем функциональным областям Kaspersky Security Center.

  О новых возможностях программы вы можете узнать в Release Notes или в справке к программе.

- Если в блок параметров в новой версии плагина управления был добавлен новый параметр, то ранее заданный статус атрибута / для этого блока параметров не изменяется.

Интерфейс программы

В главном окне Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready находятся элементы интерфейса, предоставляющие вам доступ к основным функциям программы.

Главное окно программы содержит следующие элементы:

- Ссылка Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Windows. При нажатии на ссылку открывается окно О программе со сведениями о версии программы.

- Кнопка ⓘ. При нажатии на кнопку осуществляется переход к справочной системе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

- Блок Технологии обнаружения угроз. Блок содержит следующую информацию:

  - В левой части блока отображается список технологий обнаружения угроз. Справа от названия каждой из технологий обнаружения угроз отображается количество угроз, обнаруженных с помощью этой технологии.

  - В центре блока в зависимости от наличия активных угроз отображается одна из следующих надписей:

    - Нет угроз. Если отображается эта надпись, то при нажатии на блок Технологии обнаружения угроз открывается окно Технологии обнаружения угроз, в котором приведено краткое описание технологий обнаружения угроз, а также статус и глобальная статистика инфраструктуры облачных служб Kaspersky Security Network.

    - N активных угроз. Если отображается эта надпись, то при нажатии на блок Технологии обнаружения угроз открывается окно Активные угрозы, в котором приведен список событий, связанных с зараженными файлами, которые по каким-либо причинам не были обработаны.

- Блок Компоненты защиты. При нажатии на блок открывается окно Компоненты защиты. В этом окне вы можете посмотреть статус работы установленных компонентов. Также из этого окна вы можете для любого из установленных компонентов, кроме компонентов шифрования, открыть подраздел в окне Настройка, содержащий параметры этого компонента.

- Блок Задачи. При нажатии на блок открывается окно Задачи. В этом окне вы можете управлять работой задач Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, посредством которых обеспечивается актуальность баз и модулей программы, выполняется проверка на присутствие вирусов или других программ, представляющих угрозу, а также выполняется проверка целостности.

- Кнопка Отчеты. При нажатии на кнопку открывается окно Отчеты, содержащее информацию о событиях, произошедших в ходе работы программы в целом, работы отдельных компонентов и выполнения задач.

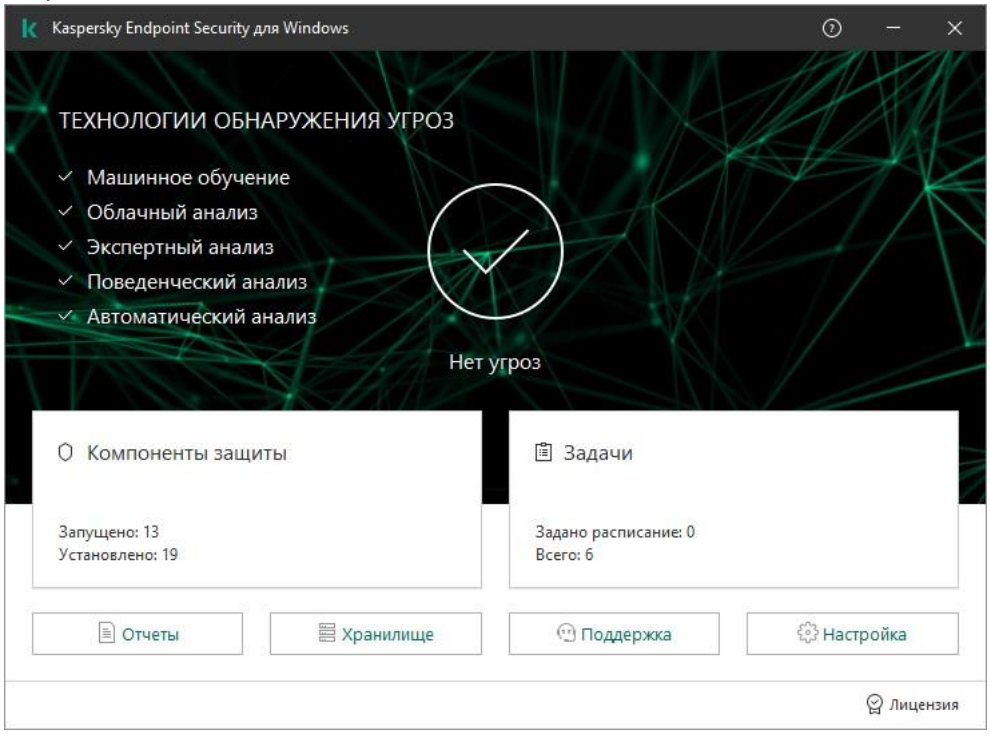
- Кнопка Хранилища. При нажатии на кнопку открывается окно Резервное хранилище. В этом окне вы можете просмотреть список копий зараженных файлов, которые были удалены в ходе работы программы.

- Кнопка Поддержка. При нажатии на кнопку открывается окно Поддержка с информацией об операционной системе, текущей версии Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и ссылками на информационные ресурсы "Лаборатории Касперского".

- Кнопка Настройка. При нажатии на кнопку открывается окно Настройка, в котором вы можете изменять параметры программы, установленные по умолчанию.

- Кнопка / / . При нажатии на кнопку открывается окно События с информацией о доступных обновлениях, а также с запросами доступа к зашифрованным файлам и устройствам.

- Ссылка Лицензия. При нажатии на ссылку открывается окно Лицензирование с информацией о действующей лицензии.



Главное окно программы

Значок программы в области уведомлений

Сразу после установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready значок программы появляется в области уведомлений панели задач Microsoft Windows.

Значок программы выполняет следующие функции:

- служит индикатором работы программы;

  обеспечивает доступ к контекстному меню значка программы и главному окну программы.

Для отображения информации о работе программы предназначены следующие статусы значка программы:

- Значок означает, что работа критически важных компонентов защиты программы включена. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready покажет предупреждение , если от пользователя требуется выполнить действие, например, перезагрузить компьютер после обновления программы.

- Значок означает, что работа критически важных компонентов защиты программы выключена или нарушена. Работа компонентов защиты может быть нарушена, например, если срок действия лицензии истек или произошел сбой в работе программы. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready покажет предупреждение с описанием проблемы в защите компьютера.

Контекстное меню значка программы содержит следующие пункты:

- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows. Открывает главное окно программы. В этом окне вы можете регулировать работу компонентов и задач программы, просматривать статистику об обработанных файлах и обнаруженных угрозах.

- Настройка. Открывает окно настройки параметров программы.

- Приостановка защиты и контроля / Возобновление защиты и контроля. Приостановка работы всех компонентов защиты и контроля, не отмеченных в политике замком ( ). Перед выполнением этой операции рекомендуется выключить политику Kaspersky Security Center.

  Перед приостановкой работы компонентов защиты и контроля программа запрашивает пароль доступа к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (пароль учетной записи или временный пароль). Далее вы можете выбрать период приостановки: на указанное время, до перезагрузки или по требованию пользователя.

  Этот пункт контекстного меню доступен, если включена Защита паролем. Для возобновления работы компонентов защиты и контроля выберите пункт Возобновление защиты и контроля в контекстном меню программы.

  > Приостановка работы компонентов защиты и контроля не влияет на выполнение задач обновления и проверки. Также программа продолжает использование Kaspersky Security Network.

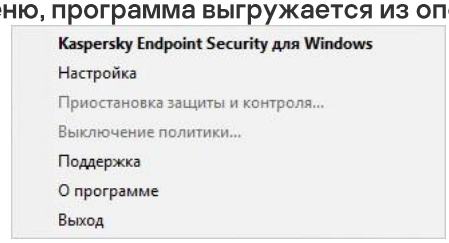
- Выключение политики / Включение политики. Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком ( ). При выключении политики программа запрашивает пароль доступа к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (пароль учетной записи или временный пароль). Этот пункт

- контекстного меню доступен, если включена Защита паролем. Для включения политики выберите пункт Включение политики в контекстном меню программы.

- Поддержка. Вызов окна Поддержка, содержащего информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".

- О программе. Открывает информационное окно со сведениями о программе.

- Выход. Завершает работу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если вы выбрали этот пункт контекстного меню, программа выгружается из оперативной памяти компьютера.

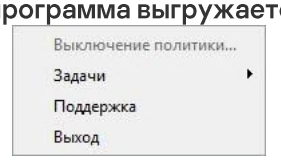


Контекстное меню значка программы

Упрощенный интерфейс программы

Если к клиентскому компьютеру, на котором установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, применена политика Kaspersky Security Center, в которой настроено отображение упрощенного интерфейса программы, то на этом клиентском компьютере недоступно главное окно программы. По правой клавише мыши пользователь может открыть контекстное меню значка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (см. рис. ниже), содержащее следующие пункты:

- Выключение политики / Включение политики. Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (). При выключении политики программа запрашивает пароль доступа к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем. Для включения политики выберите пункт Включение политики в контекстном меню программы.
- Задачи. Раскрывающийся список, содержащий следующие элементы:
  - Обновление.
  - Откат последнего обновления.
  - Полная проверка.
  - Выборочная проверка.
  - Проверка важных областей.
  - Проверка целостности.
- Поддержка. Вызов окна Поддержка, содержащего информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".
- Выход. Завершает работу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если вы выбрали этот пункт контекстного меню, программа выгружается из оперативной памяти компьютера.



Контекстное меню значка программы при отображении упрощенного интерфейса программы

Настройка отображения интерфейса программы

Вы можете настроить отображение интерфейса программы для пользователя компьютера. Пользователь может взаимодействовать с программой следующими способами:

- С упрощенным интерфейсом. На клиентском компьютере недоступно главное окно программы, а доступен только значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Также Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready показывает уведомления над значком программы.

- С полным интерфейсом. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Также Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready показывает уведомления над значком программы.

- Без интерфейса. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Также недоступны значок в области уведомлений Windows и уведомления.

Как настроить отображение интерфейса программы в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Общие параметры → Интерфейс.
6. В блоке Взаимодействие с пользователем выполните одно из следующих действий:
   - Установите флажок Отображать интерфейс программы, если вы хотите, чтобы на клиентском компьютере отображались следующие элементы интерфейса:
     - папка с названием программы в меню Пуск; значок Kaspersky Endpoint Security для
     - бизнеса – Расширенный EDR Ready в области уведомлений панели задач Microsoft
     - Windows; всплывающие уведомления.

     Если установлен этот флажок, пользователь может просматривать и, при наличии прав, изменять параметры программы из интерфейса программы.
   - Снимите флажок Отображать интерфейс программы, если вы хотите скрыть все признаки работы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready на клиентском компьютере.
7. В блоке Взаимодействие с пользователем установите флажок Упрощенный интерфейс программы, если вы хотите, чтобы на клиентском компьютере с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready отображался упрощенный интерфейс программы.

Как настроить отображение интерфейса программы в Web Console и Cloud Console

1. В главном окне Web Console выберите закладку Устройства → Политики и профили политик.

2. Нажмите на название политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для компьютеров, на которых вы хотите включить поддержку портативного режима.

   Откроется окно свойств политики.

3. Выберите закладку Параметры программы.

4. Перейдите в раздел Общие параметры → Интерфейс.

5. В блоке Взаимодействие с пользователем настройте отображение интерфейса программы:

   - С упрощенным интерфейсом. На клиентском компьютере недоступно главное окно программы, а доступен только значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready показывает уведомления над значком программы.

   - С полным интерфейсом. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready показывает уведомления над значком программы.

   - Без интерфейса. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Также недоступны значок в области уведомлений Windows и уведомления.

6. Нажмите на кнопку OK.

Подготовка программы к работе

После развертывания программы на клиентских компьютерах для работы с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из Kaspersky Security Center вам нужно выполнить следующие действия:

- Создать и настроить политику.

  При помощи политик вы можете установить одинаковые значения параметров работы программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для всех клиентских компьютеров, входящих в состав группы
  администрирования. Мастер первоначальной настройки Kaspersky Security Center создает политику для Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически.

- Создать задачи Обновление и Антивирусная проверка.

  Задача Обновление требуется для поддержания защиты компьютера в актуальном состоянии. При выполнении задачи Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обновляет антивирусные базы и модули программы. Задача Обновление создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи Обновления во время работы мастера установите веб-плагин Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows.

  Задача Антивирусная проверка требуется для своевременного обнаружения вирусов и других программ, представляющих угрозу. Задачу Антивирусная проверка вам нужно создать вручную.

Как создать задачу Поиск вирусов в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Новая задача.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Windows (11.4.0) → Поиск вирусов.

Шаг 2. Область проверки

Создайте список объектов, которые Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready будет проверять во время выполнения задачи проверки.

Шаг 3. Действие Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready

Выберите действие при обнаружении угрозы:

- Лечить; удалять, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready их удаляет.

- Лечить; информировать, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready добавляет информацию об обнаруженных зараженных файлах в список активных угроз.

- Информировать. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready добавляет информацию об этих файлах в список активных угроз.

- Выполнять лечение активного заражения немедленно. Если флажок установлен, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready использует технологию лечения активного заражения во время проверки.

  Технология лечения активного заражения направлена на лечение операционной системы от вредоносных программ, которые уже запустили свои процессы в оперативной памяти и мешают Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready удалить их с помощью других методов. В результате угроза нейтрализуется. В процессе процедуры лечения активного заражения не рекомендуется запускать новые процессы или редактировать реестр операционной системы. Технология лечения активного заражения требует значительных ресурсов операционной системы, что может замедлить работу других программ. После окончания процедуры лечения активного заражения Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready перезагружает компьютер без запроса у пользователя подтверждения.

Настройте режим запуска проверки с помощью флажка Выполнять проверку во время простоя компьютера. Флажок включает / выключает функцию, которая приостанавливает задачу Поиск вирусов, если ресурсы компьютера заняты. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready приостанавливает задачу Поиск вирусов, если не включена экранная заставка и разблокирован компьютер.

Шаг 4. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 5. Выбор учетной записи для запуска задачи

Выберите учетную запись для запуска задачи Поиск вирусов. По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запускает задачу с правами учетной записи локального пользователя. Если в область проверки входят сетевые диски или другие объекты, доступ к которым ограничен, выберите учетную запись пользователя с необходимыми правами доступа.

Шаг 6. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или после загрузки антивирусных баз в хранилище.

Шаг 7. Определение названия задачи

Введите название задачи, например, `Полная проверка каждый день`.

Шаг 8. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок Запустить задачу после завершения работы мастера. Вы можете следить за ходом выполнения задачи в свойствах задачи. В результате на компьютерах пользователей будет выполняться антивирусная проверка в соответствии с установленным расписанием.

Как создать задачу Антивирусная проверка в Web Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Добавить.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке Программа выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).

   b. В раскрывающемся списке Тип задачи выберите Антивирусная проверка.

   c. В поле Название задачи введите короткое описание, например, Еженедельная проверка.

   d. В блоке Выбор устройств, которым будет назначена задача выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку Далее.

5. Завершите работу мастера по кнопке Готово.

   В списке задач отобразится новая задача.

6. Для настройки расписания выполнения задачи перейдите в свойства задачи.

   Рекомендуется настроить расписание выполнения задачи минимум раз в неделю.

7. Установите флажок напротив задачи.

8. Нажмите на кнопку Запустить.

   Вы можете отслеживать статус задачи, количество устройств, на которых задача выполнена успешно или завершилась с ошибкой.

В результате на компьютерах пользователей будет выполняться антивирусная проверка в соответствии с установленным расписанием.

Управление политиками

Политика – это набор параметров работы программы, определенный для группы администрирования. Для одной программы можно настроить несколько политик с различными значениями. Для разных групп администрирования параметры работы программы могут быть различными. В каждой группе администрирования может быть создана собственная политика для программы.

Параметры политики передаются на клиентские компьютеры с помощью Агента администрирования при синхронизации. По умолчанию Сервер администрирования выполняет синхронизацию сразу после изменения параметров политики. Синхронизация выполняется через UDP-порт 15000 на клиентском компьютере. Сервер администрирования по умолчанию выполняет синхронизацию каждые 15 минут. Если синхронизация после изменения параметров политики не удалась, следующая попытка синхронизации будет выполнена по настроенному расписанию.

Активная и неактивная политика

Политика предназначена для группы управляемых компьютеров и может быть активной или неактивной. Параметры активной политики во время синхронизации сохраняются на клиентских компьютерах. К одному компьютеру нельзя одновременно применить несколько политик, поэтому в каждой группе активной может быть только одна политика.

Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры программы на компьютерах в сети. Неактивные политики предназначены для подготовки к нештатным ситуациям, например, в случае вирусной атаки. В случае атаки через флеш-накопители, вы можете активировать политику, блокирующую доступ к флеш-накопителям. При этом активная политика автоматически становится неактивной.

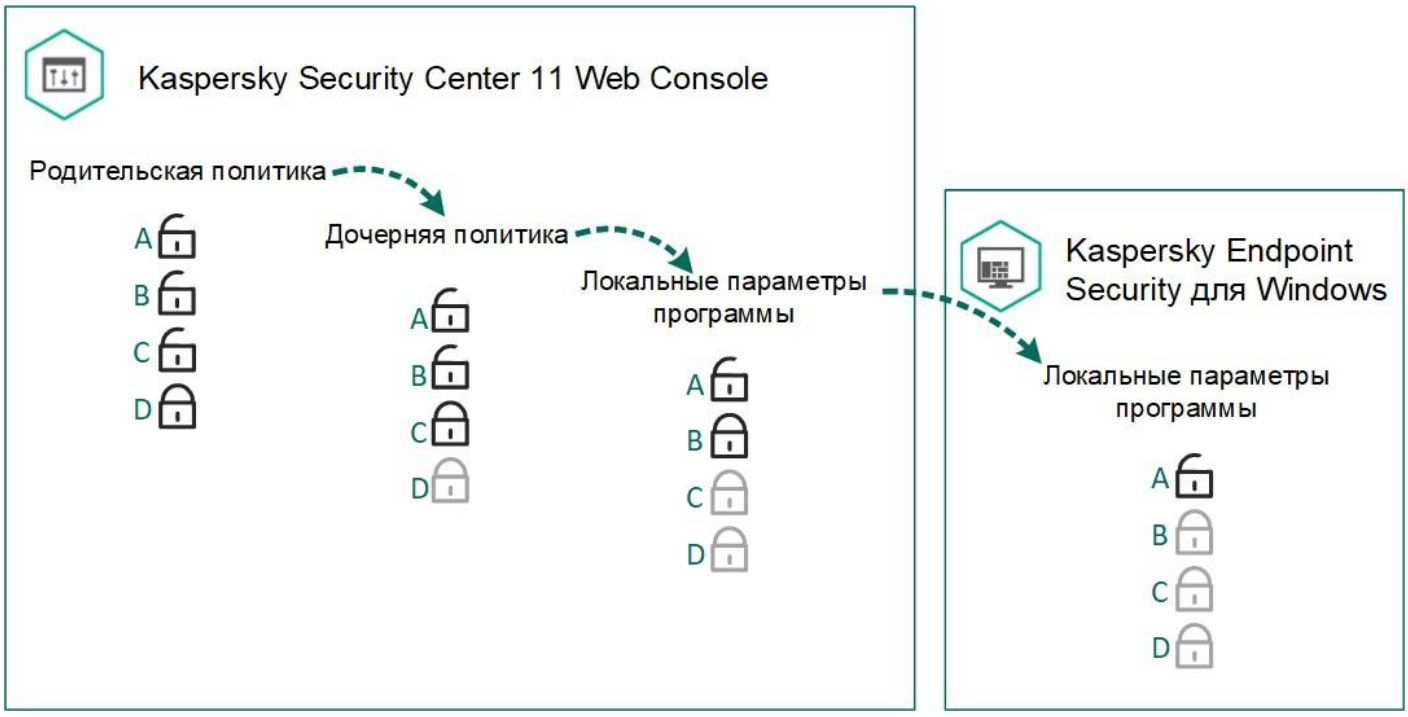
Политика для автономных пользователей

Политика для автономных пользователей активируется, когда компьютер покидает периметр сети организации.

Наследование параметров

Политики, как и группы администрирования, имеют иерархию. По умолчанию дочерняя политика наследует параметры родительской политики. Дочерняя политика – политика вложенного уровня иерархии, т.е. политика для вложенных групп администрирования и подчиненных Серверов администрирования. Вы можете выключить наследование параметров из родительской политики.

Каждый параметр, представленный в политике, имеет атрибут, который показывает, наложен ли запрет на изменение параметров в дочерних политиках и локальных параметрах программы. Атрибут работает только, если в дочерней политике включено наследование параметров из родительской политики. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.



Наследование параметров

Права на доступ к параметрам политики (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, и отдельно для каждой функциональной области Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Для настройки прав доступа к параметрам политики перейдите в раздел Безопасность окна свойств Сервера администрирования Kaspersky Security Center.

Создание политики

Как создать политику в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят интересующие вас клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Нажмите на кнопку Новая политика.

   Запустится мастер создания политики.
5. Следуйте указаниям мастера создания политики.

Как создать политику в Web Console и Cloud Console

1. В главном окне Web Console выберите Устройства → Политики и профили политик.

2. Нажмите на кнопку Добавить.

   Запустится мастер создания политики.

3. Выберите программу Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и нажмите Далее.

4. Прочитайте и примите условия Положения о Kaspersky Security Network (KSN) и нажмите Далее.

5. На закладке Общие вы можете выполнить следующие действия:

   - Изменить имя политики.
   - Выбрать состояние политики:
     - Активна. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.
     - Неактивна. Резервная политика. При необходимости неактивную политику можно сделать активной.
     - Для автономных пользователей. Политика начинает действовать, когда компьютер покидает периметр сети организации.
   - Настроить наследование параметров:
     - Наследовать параметры родительской политики. Если переключатель включен, значения параметров политики наследуются из политики верхнего уровня иерархии. Параметры политики недоступны для изменения, если в родительской политике установлен.
     - Обеспечить принудительное наследование параметров для дочерних политик. Если переключатель включен, значения параметров политики будут распространены на дочерние политики. В свойствах дочерней политики будет автоматически включен и недоступен для выключения переключатель Наследовать параметры родительской политики. Параметры дочерней политики наследуются из родительской политики, кроме параметров с . Параметры дочерних политик недоступны для изменения, если в родительской политике установлен.

6. На закладке Параметры программ вы можете настроить параметры политики Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

7. Нажмите на кнопку Сохранить.

В результате параметры Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready будут настроены на клиентских компьютерах при следующей синхронизации. Вы можете просмотреть информацию о политике, которая применена к компьютеру, в интерфейсе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready по кнопке Поддержка на главном экране (например, имя политики). Для этого в параметрах политики Агента администрирования нужно включить получение расширенных данных политики. Подробнее о политике Агента администрирования см. в справке Kaspersky Security Center.

Индикатор уровня защиты

В верхней части окна Свойства: <Название политики> отображается индикатор уровня защиты. Индикатор может принимать одно из следующих значений:

- Уровень защиты высокий. Индикатор принимает это значение и цвет индикатора изменяется на зеленый, если включены все компоненты, относящиеся к следующим категориям:
  - Критические. Категория включает следующие компоненты:
    - Защита от файловых угроз.
    - Анализ поведения.
    - Защита от эксплойтов.
    - Откат вредоносных действий.
  - Важные. Категория включает следующие компоненты:
    - Kaspersky Security Network.
    - Защита от веб-угроз.
    - Защита от почтовых угроз.
    - Предотвращение вторжений.
- Уровень защиты средний. Индикатор принимает это значение и цвет индикатора изменяется на желтый, если отключен один важный компонент.
- Уровень защиты низкий. Индикатор принимает это значение и цвет индикатора изменяется на красный в одном из следующих случаев:
  - отключены один или несколько критических компонентов;
  - отключены два или более важных компонента.

Если отображается индикатор со значением Уровень защиты средний или Уровень защиты низкий, то справа от индикатора доступна ссылка, по которой открывается окно Рекомендованные компоненты защиты. В этом окне вы можете включить любой из рекомендованных компонентов защиты.

Управление задачами

Для работы с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного клиентского компьютера; групповые задачи,
- определенные для клиентских компьютеров, входящих в группы администрирования; задачи для
- выборки компьютеров.

Вы можете создавать любое количество групповых задач, задач для выборки компьютеров и локальных задач. Подробнее о работе с группами администрирования и выборками компьютеров см. в справке Kaspersky Security Center.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает выполнение следующих задач:

- Антивирусная проверка. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи. Задача Антивирусная проверка является обязательной для работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и создается во время работы мастера первоначальной настройки. Рекомендуется настроить расписание выполнения задачи минимум раз в неделю.

- Добавление ключа. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавляет ключ для активации программ, в том числе дополнительный. Перед выполнением задачи убедитесь, что количество компьютеров, на которых будет выполняться задача, не превышает количество компьютеров, на которые рассчитана лицензия.

- Изменение состава компонентов программы. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready устанавливает или удаляет на клиентских компьютерах компоненты согласно списку компонентов, указанному в параметрах задачи. Компонент Защита от файловых угроз удалить невозможно. Оптимальный состав компонентов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет экономить ресурсы компьютера.

- Инвентаризация. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready получает информацию обо всех исполняемых файлах программ, хранящихся на компьютерах. Задачу Инвентаризация выполняет компонент Контроль программ. Если компонент Контроль программ не установлен, задача завершит работу с ошибкой.

- Обновление. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обновляет базы и модули программы. Задача Обновление является обязательной для работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и создается во время работы мастера первоначальной настройки. Рекомендуется настроить расписание выполнения задачи минимум раз в день.

- Удаление данных. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет файлы и папки с компьютеров пользователей немедленно или при длительном отсутствии связи с Kaspersky Security Center.

- Откат обновления. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready откатывает последнее обновление баз и модулей программы. Это может понадобиться, например, если новые базы содержат некорректные данные, из-за которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может блокировать безопасную программу.

- Проверка целостности. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready анализирует файлы программы, проверяет файлы на наличие повреждений или изменений и проверяет цифровые подписи файлов программы.

- Управление учетными записями Агента аутентификации. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready настраивает параметры учетных записей Агента аутентификации. Агент аутентификации нужен для работы с зашифрованными дисками. Перед загрузкой операционной системы пользователю нужно пройти аутентификацию с помощью агента.

Запуск задач на компьютере выполняется только в том случае, если запущена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Создание задачи

Как создать задачу в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку Задачи дерева Консоли администрирования.
3. Нажмите на кнопку Новая задача.

   Запустится мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.

Как создать задачу в Web Console и Cloud Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.
2. Нажмите на кнопку Добавить.

   Запустится мастер создания задачи.
3. Настройте параметры задачи:
   a. В раскрывающемся списке Программа выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).
   b. В раскрывающемся списке Тип задачи выберите задачу, которую вы хотите запустить на компьютерах пользователей.
   c. В поле Название задачи введите короткое описание, например, `Обновление программы для бухгалтерии`.
   d. В блоке Выбор устройств, которым будет назначена задача выберите область действия задачи.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку Далее.
5. Завершите работу мастера по кнопке Готово.

В списке задач отобразится новая задача. Задача будет иметь параметры по умолчанию. Для настройки параметров задачи вам нужно перейти в свойства задачи. Для выполнения задачи вам нужно установить

флажок напротив задачи и нажать на кнопку Запустить. После запуска задачи вы можете остановить задачу и возобновить выполнение задачи позже.

В списке задач вы можете контролировать результат выполнения задачи: статус задачи и статистику выполнения задачи на компьютерах. Также вы можете создать выборку событий для контроля за выполнением задач (Мониторинг и отчеты → Выборки событий). Подробнее о выборке событий см. в справке Kaspersky Security Center. Также результаты выполнения задач сохраняются локально на компьютере в журнале событий Windows и в отчетах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Управление доступом к задачам

Права на доступ к задачам Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Для настройки доступа к функциональным областям Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready перейдите в раздел Безопасность окна свойств Сервера администрирования Kaspersky Security Center. Подробнее о концепции управления задачами через Kaspersky Security Center см. в справке Kaspersky Security Center.

Вы можете настроить права доступа к задачам для пользователей компьютеров с помощью политики (режим работы с задачами). Например, вы можете скрыть групповые задачи в интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Как настроить режим работы с задачами в интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку Политики.

4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

5. В окне политики выберите Локальные задачи → Управление задачами.

6. В блоке Управление задачами выполните следующие действия:

   - Если вы хотите разрешить пользователям работу с локальными задачами в интерфейсе и командной строке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, установите флажок Разрешить использование локальных задач.

     Если флажок снят, функционирование локальных задач прекращается. В этом режиме локальные задачи не запускаются по расписанию. Также локальные задачи недоступны для запуска и редактирования в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и при работе с командной строкой.

   - Если вы хотите разрешить пользователям просматривать список групповых задач, установите флажок Разрешить отображение групповых задач.

   - Если вы хотите разрешить пользователям изменять параметры групповых задач, установите флажок Разрешить управление групповыми задачами.

7. Сохраните внесенные изменения.

Как настроить режим работы с задачами в интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через Web Console

1. В главном окне Web Console выберите закладку Устройства → Политики и профили политик.
2. Нажмите на название политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для компьютеров, на которых вы хотите включить поддержку портативного режима.

   Откроется окно свойств политики.
3. Выберите закладку Параметры программы.
4. Перейдите в раздел Локальные задачи → Управление задачами.
5. Настройте режим работы с задачами (см. таблицу ниже).
6. Нажмите на кнопку OK.
7. Подтвердите изменения по кнопке Сохранить.

Параметры управления задачами

Параметр	Описание
Разрешить использование локальных задач	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Пользователь, при отсутствии дополнительных ограничений политики, может настраивать и запускать задачи. Если флажок снят, то использование локальных задач прекращается. В этом режиме локальные задачи не запускаются по расписанию. Задачи недоступны для запуска и настройки в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, а также при работе с командной строкой. Пользователь по-прежнему может запустить антивирусную проверку файла или папки, выбрав пункт Проверить на вирусы в контекстном меню файла или папки. При этом задача проверки запустится со значениями параметров, установленными по умолчанию для задачи выборочной проверки.
Разрешить отображение групповых задач	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Пользователь может просмотреть полный список задач в интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready показывает пустой список задач.
Разрешить управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в Kaspersky Security Center групповые задачи. Пользователь может запускать и останавливать задачи в интерфейсе программы или в упрощенном интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в Kaspersky Security Center.

Настройка локальных параметров программы

В Kaspersky Security Center вы можете настроить параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на конкретном компьютере – локальные параметры программы. Некоторые параметры могут быть недоступны для изменения. Эти параметры заблокированы атрибутом в свойствах политики.

Как настроить локальные параметры программы в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку Устройства.
4. Выберите компьютер, для которого вы хотите настроить параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
5. В контекстном меню клиентского компьютера выберите пункт Свойства.

   Откроется окно свойств клиентского компьютера.
6. В окне свойств клиентского компьютера выберите раздел Программы.

   Справа в окне свойств клиентского компьютера отобразится список программ "Лаборатории Касперского", установленных на клиентском компьютере.
7. Выберите программу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
8. Нажмите на кнопку Свойства под списком программ "Лаборатории Касперского".

   Откроется окно Параметры программы "Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows".
9. В разделе Общие параметры настройте параметры работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, а также параметры отчетов и хранилищ.

   Остальные разделы окна Параметры программы "Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows" стандартны для программы Kaspersky Security Center. Описание этих разделов вы можете прочитать в справке для Kaspersky Security Center.

   Если для программы создана политика, в которой запрещено изменение некоторых параметров, то во время настройки параметров программы в разделе Общие параметры их изменение недоступно.
10. В окне Параметры программы "Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows" нажмите на кнопку OK, чтобы сохранить внесенные изменения.

Как настроить локальные параметры программы в Web Console и Cloud Console

1. В главном окне Web Console выберите Устройства → Управляемые устройства.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры программы.
   Откроются свойства компьютера.
3. Выберите закладку Программы.
4. Нажмите на Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows.
   Откроются локальные параметры программы
5. Выберите закладку Параметры программы.
6. Настройте локальные параметры программы.
7. Локальные параметры программы повторяют параметры политики, кроме параметров шифрования.

Запуск и остановка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready

После установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на компьютер пользователя запуск программы выполняется автоматически. Далее по умолчанию запуск Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняется сразу после операционной системы. Настроить автоматический запуск программы в параметрах операционной системы невозможно.

Загрузка антивирусных баз Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready после загрузки операционной системы занимает до двух минут, в зависимости от производительности (технических возможностей) компьютера. В течение этого времени уровень защиты компьютера снижен. Загрузка антивирусных баз при запуске программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в уже запущенной операционной системе не вызывает снижения уровня защиты компьютера.

Как настроить запуск Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Общие параметры → Параметры программы.
6. С помощью флажка Запускать Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows при включении компьютера настройте запуск программы.

7. Нажмите на кнопку Сохранить, чтобы сохранить внесенные изменения.

Как настроить запуск Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в Web Console

1. В главном окне Web Console выберите Устройства → Политики и профили политик.
2. Нажмите на название политики Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для компьютеров, на которых вы хотите настроить запуск программы.

Откроется окно свойств политики.

3. Выберите закладку Параметры программы.
4. Выберите раздел Общие параметры.
5. Перейдите по ссылке Параметры программы.
6. С помощью флажка Запускать Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Windows при включении компьютера настройте запуск программы.
7. Нажмите на кнопку OK.
8. Подтвердите изменения по кнопке Сохранить.

Как настроить запуск Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в интерфейсе программы

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры программы.
3. С помощью флажка Запускать Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Windows при включении компьютера настройте запуск программы.
4. Нажмите на кнопку Сохранить, чтобы сохранить внесенные изменения.

Специалисты "Лаборатории Касперского" рекомендуют не завершать работу Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, поскольку в этом случае защита компьютера и ваших данных окажется под угрозой. Если требуется, вы можете приостановить защиту компьютера на необходимый срок, не завершая работу программы.

Вы можете контролировать статус работы программы с помощью виджета Состояние защиты.

Как запустить или остановить Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку Устройства.
4. Выберите компьютер, на котором вы хотите запустить или остановить программу.
5. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт Свойства.
6. В окне свойств клиентского компьютера выберите раздел Программы.

   Справа в окне свойств клиентского компьютера отобразится список программ "Лаборатории Касперского", установленных на клиентском компьютере.
7. Выберите программу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
8. Выполните следующие действия:
   - Если вы хотите запустить программу, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  .
   - Если вы хотите остановить работу программы, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  .

Как запустить или остановить Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в Web Console

1. В главном окне Web Console выберите Устройства → Управляемые устройства.
2. Нажмите на имя компьютера, на котором вы хотите запустить или остановить Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Откроется окно свойств компьютера.

3. Выберите закладку Программы.
4. Установите флажок напротив программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows.
5. Нажмите на кнопку Запустить или Остановить.

Как запустить или остановить Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через командную строку

Для завершения работы программы из командной строки необходимо выключить внешнее управление системными службами.

Для запуска или завершения работы программы из командной строки используется файл klpsm.exe, входящий в комплект поставки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
3. Для запуска программы в командной строке введите `klpsm.exe start_avp_service`.
4. Для остановки программы в командной строке введите `klpsm.exe stop_avp_service`.

Приостановка и возобновление защиты и контроля компьютера

Приостановка защиты и контроля компьютера означает выключение на некоторое время всех компонентов защиты и всех компонентов контроля Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Состояние программы отображается с помощью значка программы в области уведомлений панели

- задач: значок свидетельствует о приостановке защиты и контроля компьютера; значок
- свидетельствует о том, что защита и контроль компьютера включены.

Приостановка и возобновление защиты и контроля компьютера не оказывает влияния на выполнение задач проверки и задачи обновления.

Если в момент приостановки и возобновления защиты и контроля компьютера были установлены сетевые соединения, на экран выводится уведомление о разрыве этих сетевых соединений.

Чтобы приостановить защиту и контроль компьютера, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт Приостановка защиты и контроля (см. рисунок ниже).

   Этот пункт контекстного меню доступен, если включена Защита паролем.
3. Выберите один из следующих вариантов:
   - Приостановить на указанное время – защита и контроль компьютера включатся через интервал времени, указанный в раскрывающемся списке ниже.
   - Приостановить до перезагрузки – защита и контроль компьютера включатся после перезапуска программы или перезагрузки операционной системы. Для использования этой возможности должен быть включен автоматический запуск программы.
   - Приостановить – защита и контроль компьютера включатся тогда, когда вы решите возобновить их.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready приостановит работу всех компонентов защиты и контроля, не отмеченных в политике замком (). Перед выполнением этой операции рекомендуется выключить политику Kaspersky Security Center.

Контекстное меню значка программы

Чтобы возобновить защиту и контроль компьютера, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.

2. В контекстном меню выберите пункт Возобновление защиты и контроля.

Вы можете возобновить защиту и контроль компьютера в любой момент, независимо от того, какой вариант приостановки защиты и контроля компьютера вы выбрали ранее.

Проверка компьютера

Антивирусная проверка является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять антивирусную проверку, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive, и создает в журнале записи о том, что эти файлы не были проверены.

Полная проверка

Тщательная проверка всей системы. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет следующие объекты:

- память ядра; объекты, загрузка которых осуществляется при запуске
- операционной системы; загрузочные секторы; резервное хранилище
- операционной системы; все жесткие и съемные диски.
-

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи Полная проверка.

Для экономии ресурсов компьютера рекомендуется вместо задачи полной проверки запускать задачу фоновой проверки. Уровень защиты компьютера при этом не изменится.

Проверка важных областей

По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет память ядра, запущенные процессы и загрузочные секторы.

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи Проверка важных областей.

Выборочная проверка

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет объекты, выбранные пользователем. Вы можете проверить любой объект из следующего списка:

- память ядра; объекты, загрузка которых осуществляется при запуске
- операционной системы; резервное хранилище операционной системы;
- почтовый ящик Outlook; жесткие, съемные и сетевые диски; любой
- выбранный файл.

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет объекты автозапуска, памяти ядра и системного раздела.

Проверка целостности

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет модули программы на наличие повреждений или изменений.

Запуск и остановка задачи проверки

Независимо от выбранного режима запуска задачи проверки вы можете запустить или остановить задачу проверки в любой момент.

Чтобы запустить или остановить задачу проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Задачи.
2. В открывшемся окне выберите задачу проверки.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку Запустить, если вы хотите запустить задачу проверки.

     Статус выполнения задачи, отображающийся под названием задачи проверки, изменится на Выполняется.
   - Выберите в контекстном меню пункт Остановить, если вы хотите остановить задачу проверки.

     Статус выполнения задачи, отображающийся под названием задачи проверки, изменится на Остановлена.

Чтобы запустить или остановить задачу проверки при отображении упрощенного интерфейса программы, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке Задачи выполните одно из следующих действий:

- выберите незапущенную задачу проверки, чтобы запустить ее;
- выберите запущенную задачу проверки, чтобы остановить ее; •

выберите остановленную задачу проверки, чтобы возобновить ее или

запустить ее заново.

Изменение уровня безопасности

Для выполнения задач проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready применяет разные наборы параметров. Наборы параметров, сохраненные в программе, называются уровнями безопасности. Предустановлены три уровня безопасности: Высокий, Рекомендуемый, Низкий. Параметры уровня безопасности Рекомендуемый считаются оптимальными. Они рекомендованы специалистами "Лаборатории Касперского". Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

Чтобы изменить уровень безопасности, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей или Выборочная проверка.
3. В блоке Уровень безопасности выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности (Высокий, Рекомендуемый, Низкий), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку Настройка и задайте параметры в открывшемся окне с названием задачи проверки.

     После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке Уровень безопасности изменится на Другой.
   - Если вы хотите изменить уровень безопасности на Рекомендуемый, нажмите на кнопку По умолчанию.
4. Нажмите на кнопку Сохранить, чтобы сохранить внесенные изменения.

Изменение действия над зараженными файлами

По умолчанию при обнаружении зараженных файлов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready пытается вылечить их или удаляет их, если лечение невозможно.

Чтобы изменить действие над зараженными файлами, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей, Выборочная проверка или Проверка из контекстного меню.
3. В блоке Действие при обнаружении угрозы, выберите один из следующих вариантов:
   - Установите флажок Лечить; удалять, если лечение невозможно, если вы хотите, чтобы при обнаружении зараженных файлов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready пытался вылечить их или удалял их, если лечение невозможно.
   - Установите флажок Лечить; информировать, если лечение невозможно, если вы хотите, чтобы при обнаружении зараженных файлов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready пытался вылечить их и информировал вас, если лечение невозможно.
   - Установите флажок Информировать, если вы хотите, чтобы при обнаружении зараженных файлов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready информировал вас об этом.

   При обнаружении зараженных файлов, являющихся частью приложения Windows Store, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет действие Удалить.
4. Нажмите на кнопку Сохранить, чтобы сохранить внесенные изменения.

Формирование списка проверяемых объектов

Чтобы сформировать список проверяемых объектов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей, Выборочная проверка или Проверка из контекстного меню.
3. Нажмите на кнопку Область проверки.
   Откроется окно Область проверки.
4. Если вы хотите добавить новый объект в область проверки, выполните следующие действия: a.
   Нажмите на кнопку Добавить.
   Откроется окно Выбор области проверки.
   b. Выберите объект и нажмите на кнопку Добавить.
   Все объекты, выбранные в окне Выбор области проверки, отобразятся в списке Область проверки.
   c. Нажмите на кнопку OK.
5. Если вы хотите изменить путь к объекту области проверки, выполните следующие действия:
   a. Выберите объект из области проверки.

b. Нажмите на кнопку Изменить.

Откроется окно Выбор области проверки.

c. Введите новый путь к объекту области проверки.

d. Нажмите на кнопку OK.

Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.

6. Если вы хотите удалить объект из области проверки, выполните следующие действия:

a. Выберите объект, который вы хотите удалить из области проверки.

Чтобы выбрать несколько объектов, выделяйте их, удерживая клавишу CTRL.

b. Нажмите на кнопку Удалить.

Откроется окно подтверждения удаления.

c. Нажмите на кнопку Да в окне подтверждения удаления.

Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.

7. Чтобы исключить объект из области проверки, в окне Область проверки снимите флажок рядом с ним.

Объект остается в списке объектов области проверки, но не проверяется во время выполнения задачи проверки.

8. Сохраните внесенные изменения.

Выбор типа проверяемых файлов

Выбирая тип проверяемых файлов, нужно учитывать следующее:

1. Вероятность внедрения вредоносного кода в файлы некоторых форматов и его последующей активации низка (например, формат TXT). В то же время существуют форматы файлов, которые содержат исполняемый код (например, форматы EXE, DLL). Также исполняемый код могут содержать форматы файлов, которые для этого не предназначены (например, формат DOC). Риск внедрения в такие файлы вредоносного кода и его активации высок.

2. Злоумышленник может отправить вирус или другую программу, представляющую угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки программа пропускает такой файл. Если же выбрана проверка файлов по формату, то вне зависимости от расширения компонент Защита от файловых угроз анализирует заголовок файла. Если в результате выясняется, что файл имеет формат исполняемого файла (например, EXE), то программа проверяет его.

Чтобы выбрать тип проверяемых файлов выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей, Выборочная проверка или Проверка из контекстного меню.

3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно с названием выбранной задачи проверки.

4. В окне с названием выбранной задачи проверки выберите закладку Область действия.

5. В блоке Типы файлов укажите тип файлов, которые вы хотите проверять во время выполнения выбранной задачи проверки:

   - Выберите Все файлы, если вы хотите проверять все файлы.
   - Выберите Файлы, проверяемые по формату, если вы хотите проверять файлы тех форматов, которые наиболее подвержены заражению.
   - Выберите Файлы, проверяемые по расширению, если вы хотите проверять файлы с расширениями, типичными для файлов, которые наиболее подвержены заражению.

6. Сохраните внесенные изменения.

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Этого можно достичь, если проверять только новые файлы и те файлы, что изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы. Вы можете также ограничить длительность проверки одного файла. По истечении заданного времени Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready исключает файл из текущей проверки (кроме архивов и объектов, в состав которых входит несколько файлов).

Вы также можете включить использование технологий iChecker и iSwift. Технологии iChecker и iSwift позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

Чтобы оптимизировать проверку файлов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей, Выборочная проверка или Проверка из контекстного меню.

3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне выберите закладку Область действия.

5. В блоке Оптимизация проверки выполните следующие действия:

   - Установите флажок Проверять только новые и измененные файлы.
   -

Установите флажок Пропускать файлы, если их проверка длится более и задайте длительность проверки одного файла (в секундах).

6. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие программы, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки.

Чтобы настроить проверку составных файлов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей или Выборочная проверка.

3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне выберите закладку Область действия.

5. В блоке Проверка составных файлов укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты, файлы офисных форматов, файлы почтовых форматов, защищенные паролем архивы.

6. Если в блоке Оптимизация проверки снят флажок Проверять только новые и измененные файлы, нажмите на ссылку все / новые, расположенную рядом с названием типа составного файла, чтобы выбрать, следует ли проверять все файлы этого типа или только новые файлы этого типа.

   Ссылка меняет свое значение при нажатии.

   Если флажок Проверять только новые и измененные файлы установлен, то проверяются только новые файлы.

7. Нажмите на кнопку Дополнительно.

   Откроется окно Составные файлы.

8. В блоке Ограничение по размеру выполните одно из следующих действий:

   - Если вы не хотите распаковывать составные файлы большого размера, установите флажок Не распаковывать составные файлы большого размера и в поле Максимальный размер файла укажите нужное значение.

   - Если вы хотите распаковывать составные файлы независимо от размера, снимите флажок Не распаковывать составные файлы большого размера.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок Не распаковывать составные файлы большого размера.

9. Сохраните внесенные изменения.

Использование методов проверки

Во время своей работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать вредоносные объекты, записей о которых еще нет в базах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Чтобы использовать методы проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей, Выборочная проверка или Проверка из контекстного меню.
3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне выберите закладку Дополнительно.
5. В блоке Методы проверки установите флажок Эвристический анализ, если вы хотите, чтобы программа использовала эвристический анализ во время выполнения задачи проверки. Далее при помощи ползунка задайте уровень эвристического анализа: поверхностный, средний или глубокий.
6. Сохраните внесенные изменения.

Использование технологий проверки

Чтобы использовать технологии проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей, Выборочная проверка или Проверка из контекстного меню.
3. В блоке Уровень безопасности нажмите на кнопку Настройка.

Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне выберите закладку Дополнительно.

5. В блоке Технологии проверки установите флажки около названий технологий, которые вы хотите использовать во время проверки.

6. Сохраните внесенные изменения.

Выбор режима запуска для задачи проверки

Если по каким-либо причинам запуск задачи проверки невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи проверки, как только это станет возможным.

Вы можете отложить запуск задачи проверки после старта программы для случаев, если вы выбрали режим запуска задачи проверки По расписанию и время запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready совпадает с расписанием запуска задачи проверки. Задача проверки запускается только по истечении указанного времени после старта Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Чтобы выбрать режим запуска для задачи проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей или Выборочная проверка.

3. Нажмите на кнопку Режим запуска.

   Откроется окно свойств выбранной задачи на закладке Режим запуска.

4. В блоке Режим запуска выберите режим запуска задачи: Вручную или По расписанию.

5. Если вы выбрали вариант По расписанию, задайте параметры расписания. Для этого выполните следующие действия:

   a. В раскрывающемся списке Периодичность выберите периодичность запуска задачи (Минуты, Часы, Дни, Каждую неделю, В указанное время, Каждый месяц, После запуска программы, После каждого обновления).

   b. В зависимости от выбранной периодичности настройте дополнительные параметры, которые уточняют расписание запуска задачи.

   c. Установите флажок Запускать пропущенные задачи, если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запускал при первой возможности не запущенные вовремя задачи проверки.

   > Если в раскрывающемся списке Периодичность выбран элемент Минуты, Часы, После запуска программы или После каждого обновления, то флажок Запускать пропущенные задачи недоступен.

a. Установите флажок Выполнять только во время простоя компьютера, если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready приостанавливал задачу, когда ресурсы компьютера заняты.

   Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.

6. Сохраните внесенные изменения.

Настройка запуска задачи проверки с правами другого пользователя

По умолчанию задача проверки запускается с правами учетной записи, под которой пользователь зарегистрирован в операционной системе. Однако может возникнуть необходимость запустить задачу проверки с правами другого пользователя. Вы можете указать пользователя, обладающего этими правами, в параметрах задачи проверки и запускать задачу проверки от имени этого пользователя.

Чтобы настроить запуск задачи проверки с правами другого пользователя, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Полная проверка, Проверка важных областей или Выборочная проверка.
3. Нажмите на кнопку Режим запуска.

   Откроется окно свойств выбранной задачи на закладке Режим запуска.
4. На закладке Режим запуска в блоке Пользователь установите флажок Запускать задачу с правами пользователя.
5. В поле Имя введите имя пользователя, права которого требуется использовать для запуска задачи проверки.
6. В поле Пароль введите пароль пользователя, права которого требуется использовать для запуска задачи проверки.
7. Сохраните внесенные изменения.

Проверка съемных дисков при подключении к компьютеру

Некоторые вредоносные программы используют уязвимости операционной системы для распространения через локальные сети и съемные диски. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет проверять на вирусы и другие программы, представляющие угрозу, съемные диски при их подключении к компьютеру.

Чтобы настроить проверку съемных дисков при их подключении к компьютеру, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Задачи → Проверка съемных дисков.

3. В раскрывающемся списке Действие при подключении съемного диска выберите нужное действие:

- Не проверять.
- Подробная проверка.

  В этом режиме Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет все файлы, расположенные на съемном диске, в том числе вложенные файлы внутри составных объектов.

- Быстрая проверка.

  В этом режиме Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет только потенциально заражаемые файлы, а также не распаковывает составные объекты.

4. Выполните одно из следующих действий:

- Если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверял только те съемные диски, размер которых не превышает указанного значения, установите флажок Максимальный размер съемного диска и укажите в соседнем поле значение в мегабайтах.
- Если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверял все съемные диски, снимите флажок Максимальный размер съемного диска.

5. Выполните одно из следующих действий:

- Если вы хотите, чтобы программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображала ход проверки съемных дисков в отдельном окне, установите флажок Отображать ход проверки.

  В окне проверки съемного диска пользователь может остановить проверку. Чтобы сделать проверку съемных дисков обязательной и запретить пользователю останавливать проверку, установите флажок Запретить остановку задачи проверки.

- Если вы хотите, чтобы программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запускала проверку съемных дисков в фоновом режиме, снимите флажок Отображать ход проверки.

6. Нажмите на кнопку Сохранить, чтобы сохранить внесенные изменения.

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет объекты автозапуска, памяти ядра и системного раздела. Фоновая проверка запускается в следующих случаях:

- после обновления антивирусных баз; через 30 минут
- после запуска Kaspersky Endpoint Security для бизнеса -
- Расширенный EDR Ready; каждые шесть часов; при
- простое компьютера в течение пяти и более минут.

Фоновая проверка при простое компьютера прерывается при выполнении любого из следующих условий:

- Компьютер перешел в активный режим.

  Если фоновая проверка не выполнялась более десяти дней, проверка не прерывается.

- Компьютер (ноутбук) перешел в режим питания от батареи.

При выполнении фоновой проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

Чтобы включить фоновую проверку компьютера, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Фоновая проверка.
3. Установите флажок Выполнять проверку во время простоя компьютера.
4. Нажмите на кнопку Сохранить, чтобы сохранить внесенные изменения.

Обновление баз и модулей программы

Обновление баз и модулей программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу.
Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

Для регулярного обновления требуется действующая лицензия на использование программы. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Основным источником обновлений Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready служат серверы обновлений "Лаборатории Касперского".

Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера.

Загрузка обновлений осуществляется по протоколу HTTPS. Загрузка по протоколу HTTP может осуществляться в случае, когда загрузка обновлений по протоколу HTTPS невозможна.

В процессе обновления на ваш компьютер загружаются и устанавливаются следующие объекты:

- Базы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Защита компьютера обеспечивается на основании баз данных, содержащих сигнатуры вирусов и других программ, представляющих угрозу, и информацию о способах борьбы с ними. Компоненты защиты используют эту информацию при поиске и обезвреживании зараженных файлов на компьютере. Базы регулярно пополняются записями о появляющихся угрозах и способах борьбы с ними. Поэтому рекомендуется регулярно обновлять базы.

  Наряду с базами Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

- Модули программы. Помимо баз Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, можно обновлять и модули программы. Обновления модулей программы устраняют уязвимости Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, добавляют новые функции или улучшают существующие.

В процессе обновления базы и модули программы на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули программы отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Вместе с обновлением модулей программы может быть обновлена и контекстная справка программы.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Информация о текущем состоянии баз Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображается в блоке Обновление в окне Задачи.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Схемы обновления баз и модулей программы

Обновление баз и модулей программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу.
Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

На компьютерах пользователей обновляются следующие объекты:

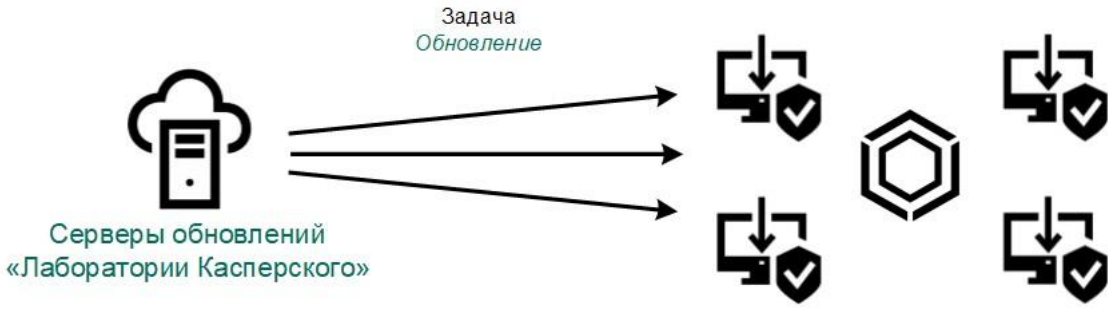
- Антивирусные базы. Антивирусные базы включают в себя базы сигнатур вредоносных программ, описание сетевых атак, базы вредоносных и фишинговых веб-адресов, базы баннеров, спам-базы и другие данные.

- Модули программы. Обновление модулей предназначено для устранения уязвимостей в программе и улучшения методов защиты компьютера. Обновления модулей могут менять поведение компонентов программы и добавлять новые возможности.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает следующие схемы обновления баз и модулей программы:

- Обновление с серверов "Лаборатории Касперского".

  Серверы обновлений "Лаборатории Касперского" расположены в разных странах по всему миру. Это обеспечивает высокую надежность обновления. Если обновление не может быть выполнено с одного сервера, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready переключается к следующему серверу.



Обновление с серверов "Лаборатории Касперского"

- Централизованное обновление.

  Централизованное обновление обеспечивает снижение внешнего интернет-трафика, а также удобство контроля за обновлением.

  Централизованное обновление состоит из следующих этапов:

  1. Загрузка пакета обновлений в хранилище внутри сети организации.

     Загрузку пакета обновлений в хранилище обеспечивает задача Сервера администрирования Загрузка обновлений в хранилище Сервера администрирования.

  2. Загрузка пакета обновлений в папку общего доступа (необязательно).

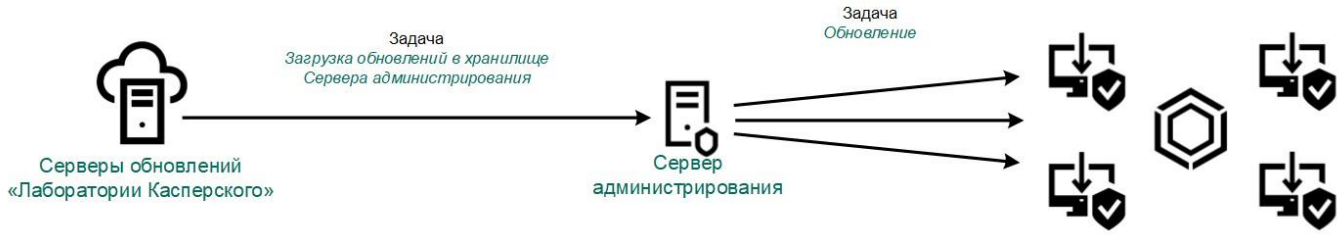
     Загрузку пакета обновлений в папку общего доступа можно обеспечить следующими способами:

     - С помощью задачи Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready Обновление. Задача предназначена для одного из компьютеров локальной сети организации.

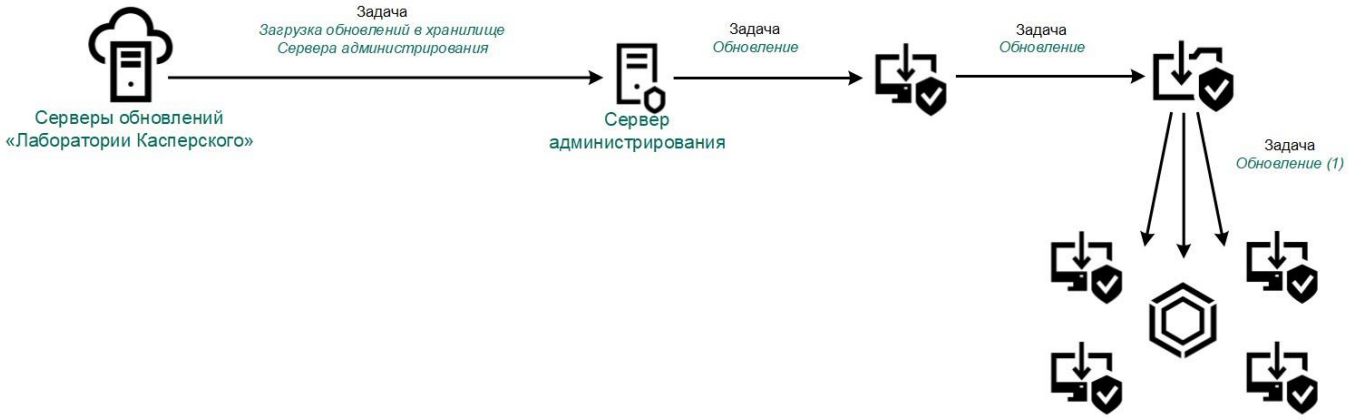
     - С помощью Kaspersky Update Utility. Подробную информацию о работе с Kaspersky Update Utility см. в Базе знаний "Лаборатории Касперского".

  3. Распространение пакета обновлений на клиентские компьютеры.

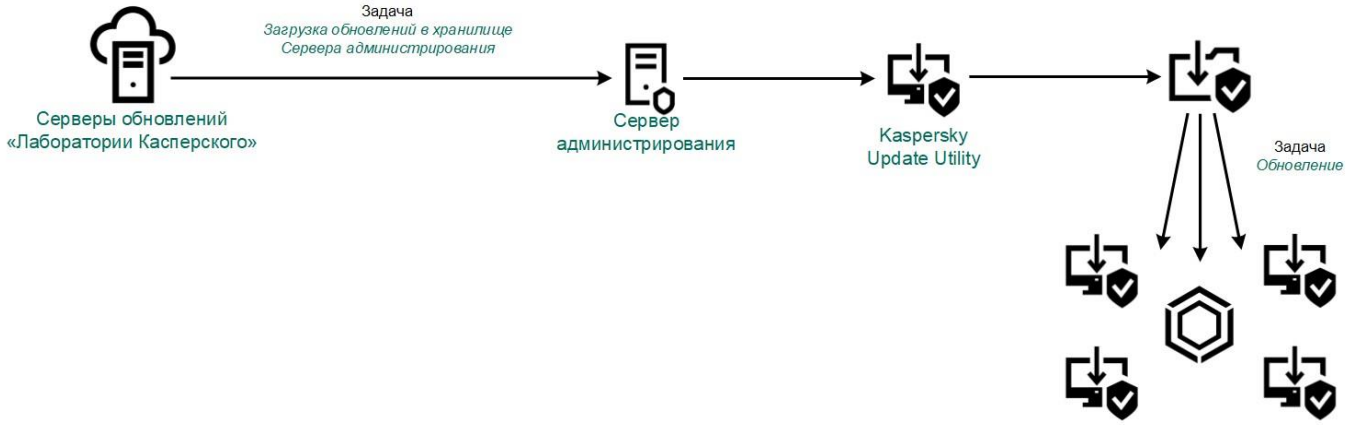
     Распространение пакета обновлений на клиентские компьютеры обеспечивает задача Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready Обновление. Вы можете создать неограниченное количество задач обновления для каждой из групп администрирования.



Обновление с серверного хранилища



Обновление из папки общего доступа



Обновление с помощью Kaspersky Update Utility

Для Web Console по умолчанию список источников обновлений содержит Сервер администрирования Kaspersky Security Center и серверы обновлений "Лаборатории Касперского". Для Kaspersky Security Center Cloud Console по умолчанию список источников обновлений содержит точки распространения и серверы обновлений "Лаборатории Касперского". Подробнее о точках распространения см. в справке Kaspersky Security Center Cloud Console. Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений можно указывать HTTP- или FTP-серверы, папки общего доступа. Если обновление не может быть выполнено с одного источника обновлений, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready переключается к следующему.

Загрузка обновлений с серверов обновлений "Лаборатории Касперского" или с других FTP- или HTTPсерверов осуществляется по стандартным сетевым протоколам. Если для доступа к источнику обновлений требуется подключение к прокси-серверу, введите параметры прокси-сервера в свойствах политики Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

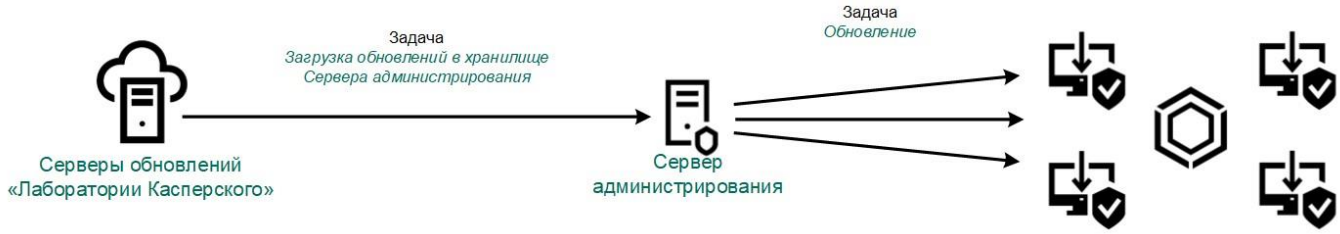
Обновление с серверного хранилища

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы на компьютерах локальной сети организации с серверного хранилища. Для этого Kaspersky Security Center должен загружать пакет обновлений в хранилище (FTP-, HTTP-сервер, сетевая или локальная папка) с серверов обновлений "Лаборатории Касперского". В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений с серверного хранилища.

Настройка обновления баз и модулей программы с серверного хранилища состоит из следующих этапов:

1. Настройка перемещения пакета обновлений в хранилище на Сервере администрирования (задача Загрузка обновлений в хранилище Сервера администрирования).

2. Настройка обновления баз и модулей программы из указанного серверного хранилища на остальных компьютерах локальной сети организации (задача Обновление).



Обновление с серверного хранилища

Чтобы настроить загрузку пакета обновлений в серверное хранилище, выполните следующие действия:

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на задачу Сервера администрирования Загрузка обновлений в хранилище Сервера администрирования.

   Откроется окно свойств задачи.

   Задача Загрузка обновлений в хранилище Сервера администрирования создается автоматически мастером первоначальной настройки Kaspersky Security Center 12 Web Console и может существовать только в единственном экземпляре.

3. Выберите закладку Параметры программы.

4. В блоке Прочие параметры нажмите на кнопку Настроить.

5. В поле Папка для хранения обновлений укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

   Формат пути для источника обновлений следующий:

   - Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.

     Например, `http://dnl-01.geo.kaspersky.com/` **или** `93.191.13.103`.
     Для FTP-сервера в адресе можно указывать параметры аутентификации в формате `ftp://<имя пользователя>:<пароль>@<узел>:<порт>`.

   - Для сетевой папки введите UNC-путь.

Например, `\\Server\Share\Update distribution`.

- Для локальной папки введите полный путь к папке.

  Например, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Сохраните внесенные изменения.

Чтобы настроить обновление Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready из указанного серверного хранилища, выполните следующие действия:

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready Обновление.

   Откроется окно свойств задачи.

   Задача Обновление создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи Обновления во время работы мастера установите веб-плагин Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Windows.

3. Выберите закладку Параметры программы → Локальный режим.

4. В списке источников обновления нажмите на кнопку Добавить.

5. В поле Источник укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

   Адрес источника должен совпадать с адресом, указанный ранее в поле Папка для хранения обновлений при настройке загрузки обновлений в серверное хранилище (см. инструкцию выше).

6. В блоке Статус выберите вариант Включено.

7. Нажмите на кнопку ОК.

8. Настройте приоритеты источников обновлений с помощью кнопок Вверх и Вниз.

9. Нажмите на кнопку Сохранить.

Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready переключается к следующему автоматически.

Обновление из папки общего доступа

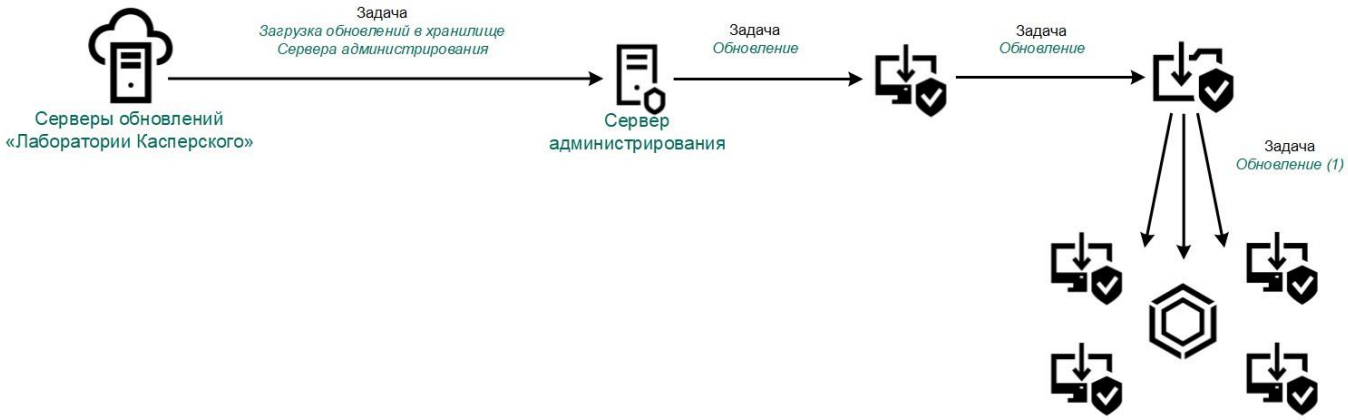
Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы на компьютерах локальной сети организации из папки общего доступа. Для этого один из компьютеров локальной сети организации должен получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или серверов обновлений "Лаборатории Касперского" и копировать полученный пакет обновлений в папку общего доступа. В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений из папки общего доступа.

Настройка обновления баз и модулей программы из папки общего доступа состоит из следующих этапов:

1. Настройка обновления баз и модулей программы с серверного хранилища.

2. Включение режима копирования пакета обновлений в папку общего доступа на одном из компьютеров локальной сети организации.

3. Настройка обновления баз и модулей программы из указанной папки общего доступа на остальных компьютерах локальной сети организации.



Обновление из папки общего доступа

Чтобы включить режим копирования пакета обновлений в папку общего доступа, выполните следующие действия:

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready Обновление.

   Откроется окно свойств задачи.

   Задача Обновление создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи Обновления во время работы мастера установите веб-плагин Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows.

3. Выберите закладку Параметры программы → Локальный режим.

4. Настройте источники обновлений.

   В качестве источников обновлений могут быть использованы серверы обновлений "Лаборатории Касперского", Сервер администрирования Kaspersky Security Center или другие FTP- или HTTP-серверы, локальные или сетевые папки.

5. Установите флажок Копировать обновления в папку.

6. В поле Расположение введите UNC-путь к папке общего доступа (например, `\\Server\Share\Update distribution`).

   Если оставить поле пустым, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет копировать пакет обновлений в папку `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

7. Нажмите на кнопку Сохранить.

Задача Обновление должна быть назначена для одного компьютера, который будет считаться источником обновлений.

Чтобы настроить обновление из папки общего доступа, выполните следующие действия:

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Добавить.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке Программа выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).

   b. В раскрывающемся списке Тип задачи выберите Обновление.

   c. В поле Название задачи введите короткое описание, например, `Обновление из папки общего доступа`.

   d. В блоке Выбор устройств, которым будет назначена задача выберите область действия задачи.

      Задача Обновление должна быть назначена остальным компьютерам локальной сети организации кроме компьютера, который считается источником обновлений.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи и нажмите на кнопку Далее.

5. Завершите работу мастера по кнопке Создать.

   В таблице задач отобразится новая задача.

6. Нажмите на созданную задачу Обновление.

   Откроется окно свойств задачи.

7. Перейдите в раздел Параметры программы.

8. Выберите закладку Локальный режим.

9. В блоке Источник обновлений нажмите на кнопку Добавить.

10. В поле Источник укажите путь к папке общего доступа.

    Адрес источника должен совпадать с адресом, указанным ранее в поле Расположение при настройке режима копирования пакета обновлений в папку общего доступа (см. инструкцию выше).

11. Нажмите на кнопку OK.

12. Настройте приоритеты источников обновлений с помощью кнопок Вверх и Вниз.

13. Нажмите на кнопку Сохранить.

Обновление с помощью Kaspersky Update Utility

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы на компьютерах локальной сети организации из папки общего доступа с помощью утилиты Kaspersky Update Utility. Для этого один из компьютеров локальной сети организации должен получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или серверов обновлений "Лаборатории Касперского" и копировать полученные пакеты обновлений в папку общего доступа с помощью утилиты. В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений из папки общего доступа.

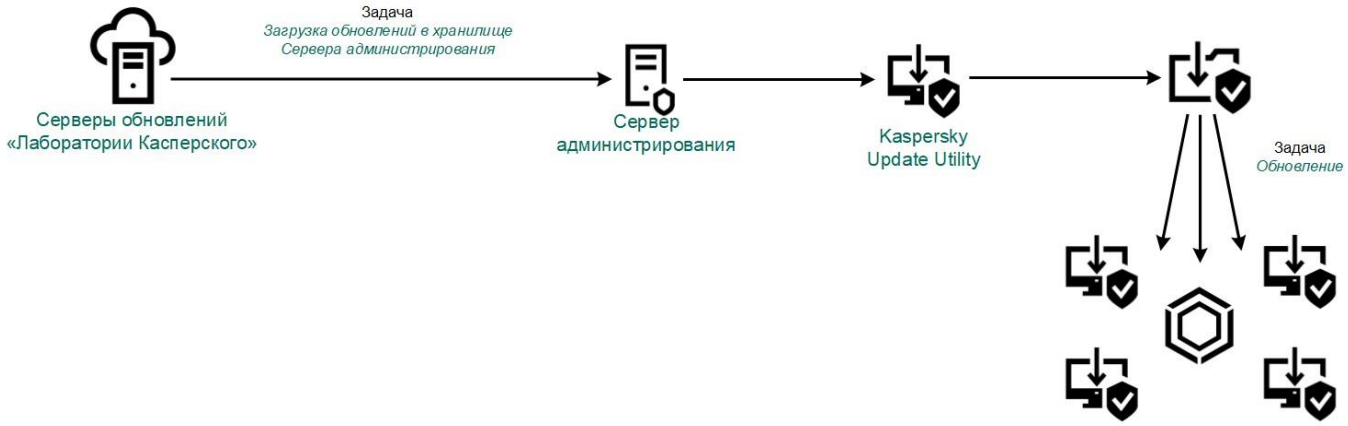
Настройка обновления баз и модулей программы из папки общего доступа состоит из следующих этапов:

1. Настройка обновления баз и модулей программы с серверного хранилища.

2. Установка Kaspersky Update Utility на одном из компьютеров локальной сети организации.

3. Настройка копирования пакета обновлений в папку общего доступа в параметрах Kaspersky Update Utility.

4. Настройка обновления баз и модулей программы из указанной папки общего доступа на остальных компьютерах локальной сети организации.



Обновление с помощью Kaspersky Update Utility

Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта Службы технической поддержки "Лаборатории Касперского". После установки утилиты выберите источник обновлений (например, хранилище Сервера администрирования) и папку общего доступа, в которую Kaspersky Update Utility будет копировать пакеты обновлений. Подробную информацию о работе с Kaspersky Update Utility см. в Базе знаний "Лаборатории Касперского".

Чтобы настроить обновление из папки общего доступа, выполните следующие действия:

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready Обновление.

   Откроется окно свойств задачи.

   Задача Обновление создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи Обновления во время работы мастера установите веб-плагин Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows.

3. Выберите закладку Параметры программы → Локальный режим.

4. В списке источников обновлений нажмите на кнопку Добавить.

5. В поле Источник введите UNC-путь к папке общего доступа (например, `\\Server\Share\Update distribution`).

   Адрес источника должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

6. Нажмите на кнопку OK.

7. Настройте приоритеты источников обновлений с помощью кнопок Вверх и Вниз.

8. Нажмите на кнопку Сохранить.

Обновление в мобильном режиме

Мобильный режим – режим работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, при котором компьютер покидает периметр сети организации (автономный компьютер). Подробнее о работе с автономными компьютерами и автономными пользователями см. в справке Kaspersky Security Center.

Автономный компьютер за пределами сети организации не может подключиться к Серверу администрирования для обновления баз и модулей программы. По умолчанию для обновления баз и модулей программы в мобильном режиме в качестве источника обновлений используются только серверы обновлений "Лаборатории Касперского". Использование прокси-сервера для подключения к интернету определяется специальной политикой для автономных пользователей. Политику для автономных пользователей требуется создать отдельно. После перехода Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в мобильный режим задача обновления запускается раз в два часа.

Чтобы настроить параметры обновления в мобильном режиме, выполните следующие действия:

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready Обновление.

   Откроется окно свойств задачи.

   Задача Обновление создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи Обновления во время работы мастера установите веб-плагин Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows.

   Выберите закладку Параметры программы → Мобильный режим.

3. Настройте источники обновлений. В качестве источников обновлений могут быть использованы серверы обновлений "Лаборатории Касперского" или другие FTP- или HTTP-серверы, локальные или сетевые папки.

4. Нажмите на кнопку Сохранить.

В результате на компьютерах пользователей будут обновлены базы и модули программы при переходе в мобильный режим.

Использование прокси-сервера при обновлении

Для загрузки обновлений баз и модулей программы из источника обновлений может потребоваться указать параметры прокси-сервера. Если источников обновлений несколько, параметры прокси-сервера применяются для всех источников. Если для некоторых источников обновлений прокси-сервер не нужен, вы можете выключить использование прокси-сервера в свойствах политики. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready также будет использовать прокси-сервер для доступа к Kaspersky Security Network и серверам активации.

Чтобы настроить подключение к источникам обновлений через прокси-сервер, выполните следующие действия:

1. В главном окне Web Console нажмите .

   Откроется окно свойств Сервера администрирования.

2. Перейдите в раздел Параметры доступа к сети Интернет.

3. Установите флажок Использовать прокси-сервер.

4. Настройте параметры подключения к прокси-серверу: адрес прокси-сервера, порт и параметры аутентификации (имя пользователя и пароль).

5. Нажмите на кнопку Сохранить.

Чтобы выключить использование прокси-сервера для определенной группы администрирования, выполните следующие действия:

1. В главном окне Web Console выберите закладку Устройства → Политики и профили политик.

2. Нажмите на название политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для компьютеров, на которых вы хотите выключить использование прокси-сервера.

   Откроется окно свойств политики.

3. Выберите закладку Параметры программы.

4. Перейдите в раздел Общие параметры → Параметры сети.

5. В блоке Параметры прокси-сервера выберите вариант Не использовать прокси-сервер.

6. Нажмите на кнопку OK.

7. Подтвердите изменения по кнопке Сохранить.

Запуск и остановка задачи обновления

Независимо от выбранного режима запуска задачи обновления вы можете запустить или остановить задачу обновления Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в любой момент.

Чтобы запустить или остановить задачу обновления, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Задачи.
2. По левой клавише мыши выберите блок с названием задачи обновления.

   Раскроется выбранный блок.
3. Выполните одно из следующих действий:

   - Выберите в меню пункт Запустить, если вы хотите запустить задачу обновления.

     Статус выполнения задачи, отображающийся под названием задачи обновления, изменится на Выполняется.
   - Выберите в меню пункт Остановить, если вы хотите остановить задачу обновления.

     Статус выполнения задачи, отображающийся под названием задачи обновления, изменится на Остановлена.

Чтобы запустить или остановить задачу обновления при отображении упрощенного интерфейса программы, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке Задачи выполните одно из следующих действий:

   - выберите незапущенную задачу обновления, чтобы запустить ее; выберите запущенную
   - задачу обновления, чтобы остановить ее; выберите остановленную задачу обновления,
   - чтобы возобновить ее или запустить ее заново.

Запуск задачи обновления с правами другого пользователя

По умолчанию задача обновления Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready может производиться из источника обновления, к которому у пользователя нет прав доступа (например, из папки общего доступа, содержащей пакет обновлений) или для которого не настроено использование аутентификации на прокси-сервере. Вы можете указать пользователя, обладающего этими правами, в параметрах Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и запускать задачу обновления Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready от имени этого пользователя.

Чтобы запускать задачу обновления с правами другого пользователя, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Обновление.
3. В блоке Режим запуска и источник обновлений нажмите на кнопку Режим запуска.

   Откроется закладка Режим запуска окна Обновление.
4. На закладке Режим запуска в блоке Пользователь установите флажок Запускать задачу с правами пользователя.
5. В поле Имя введите имя учетной записи пользователя, права которого требуется использовать для доступа к источнику обновлений.
6. В поле Пароль введите пароль пользователя, права которого требуется использовать для доступа к источнику обновлений.
7. Сохраните внесенные изменения.

Выбор режима запуска для задачи обновления

Если по каким-либо причинам запуск задачи обновления невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи обновления, как только это станет возможным.

Вы можете отложить запуск задачи обновления после старта программы для случаев, если вы выбрали режим запуска задачи обновления По расписанию и время запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready совпадает с расписанием запуска задачи обновления. Задача обновления запускается только по истечении указанного времени после старта Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Чтобы выбрать режим запуска для задачи обновления, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Обновление.
3. Нажмите на кнопку Режим запуска.

   Откроется закладка Режим запуска окна Обновление.
4. В блоке Режим запуска выберите один из следующих вариантов режима запуска задачи обновления:

   - Выберите вариант Автоматически, если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запускал задачу обновления в зависимости от наличия пакета обновлений в источнике обновления. Частота проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии.
   - Выберите вариант Вручную, если вы хотите запускать задачу обновления вручную.
   - Выберите вариант По расписанию, если вы хотите настроить расписание запуска задачи обновления.

5. Выполните одно из следующих действий:

- Если вы выбрали вариант Автоматически или Вручную, перейдите к пункту 6 инструкции.
- Если вы выбрали вариант По расписанию, задайте параметры расписания запуска задачи обновления. Для этого выполните следующие действия:

a. В раскрывающемся списке Периодичность укажите, когда следует запускать задачу обновления. Выберите один из следующих вариантов: Минуты, Часы, Дни, Каждую неделю, В указанное время, Каждый месяц, После запуска программы.

b. В зависимости от выбранного в раскрывающемся списке Периодичность элемента задайте значения параметров, которые уточняют время запуска задачи обновления.

c. В поле Отложить запуск после старта программы на укажите время, на которое следует отложить запуск задачи обновления после старта Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Если в раскрывающемся списке Периодичность выбран элемент После запуска программы, поле Отложить запуск после старта программы на недоступно.

d. Установите флажок Запускать пропущенные задачи, если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запускал при первой возможности не запущенные вовремя задачи обновления.

Если в раскрывающемся списке Периодичность выбран элемент Часы, Минуты или После запуска программы, то флажок Запускать пропущенные задачи недоступен.

6. Сохраните внесенные изменения.

Добавление источника обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Источником обновлений может быть FTP-, HTTP-сервер (например, Kaspersky Security Center, серверы обновлений "Лаборатории Касперского"), сетевая или локальная папка.

Если серверы обновлений "Лаборатории Касперского" вам недоступны (например, ограничен доступ в интернет), вы можете обратиться в центральный офис "Лаборатории Касперского" и узнать адреса партнеров "Лаборатории Касперского". Партнеры "Лаборатории Касперского" предоставят вам обновления на съемном диске.

Заказывая обновления на съемном диске, вам следует уточнить, хотите ли вы получить обновления модулей программы.

По умолчанию список источников обновлений содержит сервер Kaspersky Security Center и серверы обновлений "Лаборатории Касперского". Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений можно указывать HTTP- или FTP-серверы, папки общего доступа.

Если в качестве источников обновлений выбрано несколько ресурсов, в процессе обновления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обращается к ним строго по списку и выполняет задачу обновления, используя пакет обновлений первого доступного источника обновлений.

Чтобы добавить источник обновлений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Обновление.
3. В блоке Режим запуска и источник обновлений нажмите на кнопку Источник обновлений.
4. На закладке Источник нажмите на кнопку Добавить.
5. В открывшемся окне укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, которая содержит пакет обновлений.

   Формат пути для источника обновлений следующий:

   - Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.

     Например, `http://dnl-01.geo.kaspersky.com/` или `93.191.13.103`.

     Для FTP-сервера в адресе можно указывать параметры аутентификации в формате `ftp://<имя пользователя>:<пароль>@<узел>:<порт>`.

   - Для сетевой папки введите UNC-путь.

     Например, `\\Server\Share\Update distribution`.

   - Для локальной папки введите полный путь к папке.

     Например, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Сохраните внесенные изменения.

Выбор региона сервера обновлений

Если в качестве источника обновлений вы используете серверы "Лаборатории Касперского", вы можете выбрать местоположение сервера обновлений "Лаборатории Касперского" для загрузки пакета обновлений. Серверы обновлений "Лаборатории Касперского" расположены в нескольких странах мира. Использование географически ближайшего к вам сервера обновлений "Лаборатории Касперского" поможет сократить время получения пакета обновлений.

По умолчанию в параметрах обновления используется информация о текущем регионе из реестра операционной системы.

Чтобы выбрать регион сервера обновлений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Обновление.
3. В блоке Режим запуска и источник обновлений нажмите на кнопку Источник обновлений.
4. На закладке Источник в блоке Региональные параметры выберите Выбрать из списка.
5. В раскрывающемся списке выберите ближайшую к вашему текущему местонахождению страну.
6. Сохраните внесенные изменения.

Настройка обновления из папки общего доступа

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы на компьютерах локальной сети организации из папки общего доступа. Для этого один из компьютеров локальной сети организации должен получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или серверов обновлений "Лаборатории Касперского" и копировать полученный пакет обновлений в папку общего доступа. В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений из папки общего доступа.

Настройка обновления баз и модулей программы из папки общего доступа состоит из следующих этапов:

1. Включение режима копирования пакета обновлений в папку общего доступа на одном из компьютеров локальной сети организации.
2. Настройка обновления баз и модулей программы из указанной папки общего доступа на остальных компьютерах локальной сети организации.

Чтобы включить режим копирования пакета обновлений в папку общего доступа, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Обновление.
3. В блоке Дополнительно установите флажок Копировать обновления в папку.
4. Введите UNC-путь к папке общего доступа (например, `\\Server\Share\Update distribution`).
5. Нажмите на кнопку Сохранить.

Чтобы настроить обновление из папки общего доступа, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Задачи → Обновление.
3. В блоке Режим запуска и источник обновлений нажмите на кнопку Источник обновлений.
4. На закладке Источник нажмите на кнопку Добавить.

5. В открывшемся окне укажите путь к папке общего доступа.

> Адрес источника должен совпадать с адресом, указанным ранее при настройке режима копирования пакета обновлений в папку общего доступа (см. инструкцию выше).

6. Нажмите на кнопку OK.

7. Настройте приоритеты источников обновлений с помощью кнопок Вверх и Вниз.

8. Сохраните внесенные изменения.

Настройка обновления модулей программы

Чтобы настроить обновление модулей программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Задачи → Обновление.

3. В блоке Дополнительно выполните одно из следующих действий:

   - Установите флажок Загружать обновления модулей программы, если вы хотите, чтобы программа включала обновления модулей программы в пакеты обновлений.

   - В противном случае снимите флажок Загружать обновления модулей программы.

4. Если на предыдущем шаге установлен флажок Загружать обновления модулей программы, укажите, при каких условиях программа будет устанавливать обновления модулей программы:

   - Выберите вариант Устанавливать критические и одобренные обновления, если вы хотите, чтобы программа устанавливала критические обновления модулей программы автоматически, а остальные обновления модулей программы – после одобрения их установки, локально через интерфейс программы или с помощью Kaspersky Security Center.

   - Выберите вариант Устанавливать только одобренные обновления, если вы хотите, чтобы программа устанавливала обновления модулей программы только после одобрения их установки, локально через интерфейс программы или с помощью Kaspersky Security Center.

5. Нажмите на кнопку Сохранить, чтобы сохранить внесенные изменения.

Настройка использования прокси-сервера

Чтобы настроить параметры прокси-сервера, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Параметры сети.

3. В блоке Прокси-сервер нажмите на кнопку Настройка.

4. В окне Параметры прокси-сервера установите флажок Использовать прокси-сервер.

5. Выберите один из следующих вариантов определения адреса прокси-сервера:

   - Автоматически определять адрес прокси-сервера.

     Этот вариант выбран по умолчанию.

   - Использовать указанные адрес и порт прокси-сервера.

6. Если вы выбрали вариант Использовать указанные адрес и порт прокси-сервера, укажите значения в полях Адрес и Порт.

7. Если вы хотите включить использование аутентификации на прокси-сервере, установите флажок Задать имя пользователя и пароль для аутентификации и укажите значения в следующих полях:

   - Имя пользователя.

     Поле для ввода имени пользователя, которое используется при аутентификации на прокси-сервере.

   - Пароль.

     Поле для ввода пароля пользователя, который используется при аутентификации на прокси-сервере.

8. Если вы хотите выключить использование прокси-сервера при обновлении баз и модулей программы из папки общего доступа, установите флажок Не использовать прокси-сервер для локальных адресов.

9. Сохраните внесенные изменения.

Откат последнего обновления

После первого обновления баз и модулей программы становится доступна функция отката к предыдущим базам и модулям программы.

Каждый раз, когда пользователь запускает обновление, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает резервную копию используемых баз и модулей программы и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущих баз и модулей программы при необходимости. Возможность отката последнего обновления полезна, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует безопасную программу.

Чтобы откатить последнее обновление, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Задачи, расположенную в нижней части главного окна программы.

   Откроется окно Задачи.

2. По левой клавише мыши выберите блок с названием задачи отката обновления.

   Раскроется выбранный блок.

3. Нажмите на кнопку Запустить.

   Запустится задача отката обновления.

Статус выполнения задачи, отображающийся под названием задачи отката обновления, изменится на Выполняется.

Чтобы запустить или остановить задачу отката обновления при отображении упрощенного интерфейса программы, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.

2. В контекстном меню в раскрывающемся списке Задачи выполните одно из следующих действий:

   - Выберите незапущенную задачу отката обновления, чтобы запустить ее.
   - Выберите запущенную задачу отката обновления, чтобы остановить ее.
   - Выберите остановленную задачу отката обновления, чтобы возобновить ее или запустить ее заново.

Работа с активными угрозами

Программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready фиксирует информацию о файлах, которые она по каким-либо причинам не обработала. Эта информация записывается в виде событий в список активных угроз.

Зараженный файл считается обработанным, если Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу, совершил одно из следующих действий с этим файлом согласно заданным настройкам программы:

- Лечить.
- Удалять.
- Удалять, если лечение невозможно.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает файл в список активных угроз, если в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready по каким-либо причинам не совершил действие с этим файлом согласно заданным настройкам программы.

Такая ситуация возможна в следующих случаях:

- Проверяемый файл недоступен (например, находится на сетевом диске или внешнем диске без прав на запись данных).
- В настройках программы для задач проверки в блоке Действие при обнаружении угрозы выбрано действие Информировать, и когда на экране отобразилось уведомление о зараженном файле, пользователь выбрал вариант Пропустить.

Вы можете выполнить одно из следующих действий:

- Вручную запустить задачу выборочной проверки файлов из списка активных угроз после обновления баз и модулей программы. После проверки статус файлов может измениться.

- Удалить записи из списка активных угроз.

Работа со списком активных угроз

Список активных угроз представлен в виде таблицы событий, связанных с зараженными файлами, которые по каким-либо причинам не были обработаны.

Вы можете выполнять следующие действия с файлами из списка активных угроз:

- просматривать список активных угроз;
- проверять из списка активных угроз, используя текущую версию баз и модулей Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready;
- восстанавливать файлы из списка активных угроз в исходные папки или в другую выбранную вами папку (в случае, если исходная папка размещения файла недоступна для записи); удалять файлы из списка
- активных угроз; открыть папку исходного размещения файла из списка активных угроз.
-

Кроме того, вы можете выполнять следующие действия, работая с табличными

- данными: фильтровать активные угрозы по значениям граф или по условиям
- сложного фильтра; использовать функцию поиска активных угроз; сортировать
- активные угрозы; изменять порядок и набор граф, отображаемых в списке
- активных угроз; группировать активные угрозы.
- Если требуется, вы можете скопировать информацию о выбранных активных угрозах в буфер обмена.

Запуск задачи выборочной проверки файлов из списка активных угроз

Вы можете вручную запустить задачу выборочной проверки зараженных файлов, которые по каким-либо причинам не были обработаны. Проверку можно запустить, например, если по какой-либо причине последняя проверка была прервана или если вы хотите повторно проверить файлы из списка активных угроз после очередного обновления баз и модулей программы.

Чтобы запустить задачу выборочной проверки файлов из списка активных угроз, выполните следующие действия:

1. В главном окне программы нажмите на блок <...> активных угроз.

   Откроется окно Активные угрозы.

2. В таблице в окне Активные угрозы выберите одну или несколько записей, относящихся к файлам, которые вы хотите проверить.

   Чтобы выбрать несколько записей, выделяйте их, удерживая клавишу CTRL.

3. Запустите задачу выборочной проверки файлов одним из следующих способов:

   - Нажмите на кнопку Перепроверить.
   - По правой клавише мыши откройте контекстное меню и выберите пункт Перепроверить.

Удаление записей из списка активных угроз

Чтобы удалить записи из списка активных угроз, выполните следующие действия:

1. В главном окне программы нажмите на блок <...> активных угроз.

   Откроется окно Активные угрозы.

2. В таблице в окне Активные угрозы выберите одну или несколько записей, которые вы хотите удалить из списка активных угроз.

   Чтобы выбрать несколько записей, выделяйте их, удерживая клавишу CTRL.

3. Удалите записи одним из следующих способов:

   - Нажмите на кнопку Удалить.
   - По правой клавише мыши откройте контекстное меню и выберите пункт Удалить.

Проверка целостности программы

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет файлы программы, находящиеся в папке установки программы, на наличие повреждений или изменений. Например, если библиотека программы имеет некорректную цифровую подпись, то такая библиотека считается поврежденной. Для проверки файлов программы предназначена задача Проверка целостности. Запускайте задачу Проверка целостности, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обнаружила вредоносный объект и не обезвредила его.

Вы можете создать задачу Проверка целостности в Kaspersky Security Center 12 Web Console и Консоли администрирования. Создать задачу в программе Kaspersky Security Center Cloud Console невозможно.

Как выполнить проверку целостности программы через Консоль администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Новая задача.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0) → Проверка целостности.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или при обнаружении вирусной атаки.

Шаг 4. Определение названия задачи

Введите название задачи, например, `Проверка целостности программы после заражения компьютера`.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок Запустить задачу после завершения работы мастера. Вы можете следить за ходом выполнения задачи в свойствах задачи. В результате Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполнит проверку целостности программы. Вы также можете настроить расписание проверки целостности программы в свойствах задачи.

Как выполнить проверку целостности программы через Web Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Добавить.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке Программа выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).

   b. В раскрывающемся списке Тип задачи выберите Проверка целостности.

   c. В поле Название задачи введите короткое описание, например, `Проверка целостности программы после заражения компьютера`.

   d. В блоке Выбор устройств, которым будет назначена задача выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку Далее.

5. Завершите работу мастера по кнопке Готово.

   В списке задач отобразится новая задача.

6. Установите флажок напротив задачи.

В результате Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполнит проверку целостности программы. Вы также можете настроить расписание проверки целостности программы в свойствах задачи.

Нарушения целостности программы могут, например, возникать в следующих случаях:

- Вредоносный объект внес изменения в файлы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. В этом случае выполните процедуру восстановления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready средствами операционной системы. После восстановления запустите полную проверку компьютера и повторите проверку целостности.

- Истек срок действия цифровой подписи. В этом случае обновите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Защита компьютера

Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready получает от служб KSN сведения о категории и репутации проверяемых файлов, а также сведения о репутации проверяемых вебадресов.

Использование Kaspersky Security Network является добровольным. Программа предлагает использовать KSN во время первоначальной настройки программы. Начать или прекратить использование KSN можно в любой момент.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского". Файл ksn_<ID языка>.txt с текстом Положения о Kaspersky Security Network входит в комплект поставки программы.

Для снижения нагрузки на серверы KSN специалисты "Лаборатории Касперского" могут выпускать обновления для программы, которые временно выключают или частично ограничивают обращения в Kaspersky Security Network. В этом случае статус подключения к KSN в локальном интерфейсе программы – Включено с ограничениями.

Инфраструктура KSN

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает следующие инфраструктурные решения KSN:

- Глобальный KSN – это решение, которое используют большинство программ "Лаборатории Касперского".

  Участники KSN получают информацию от Kaspersky Security Network, а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз Kaspersky Security Network.

- Локальный KSN – это решение, позволяющее пользователям компьютеров, на которые установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready или другие программы "Лаборатории Касперского", получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров. Локальный KSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky
  - Security Network, например, по следующим причинам: отсутствие подключения локальных рабочих мест к сети Интернет;
  -

  законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

По умолчанию Kaspersky Security Center использует Глобальный KSN. Вы можете настроить использование Локального KSN в Консоли администрирования (MMC) и Kaspersky Security Center 12 Web Console. Настроить использование Локального KSN в Kaspersky Security Center Cloud Console невозможно.

Подробнее о работе Локального KSN см. в документации для Kaspersky Private Security Network.

KSN Proxy

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал связи с внешней сетью и ускоряя получение компьютером пользователя запрошенной информации.

Подробную информацию о службе KSN Proxy см. в справке Kaspersky Security Center.

О предоставлении данных при использовании Kaspersky Security Network

Принимая Положение о Kaspersky Security Network, вы соглашаетесь передавать в автоматическом режиме следующую информацию:

- Если флажок Kaspersky Security Network установлен, а флажок Включить расширенный режим KSN снят, программа передает следующую информацию:
  - информацию об обновлении конфигурации KSN: идентификатор действующей конфигурации, идентификатор полученной конфигурации, код ошибки обновления конфигурации;
  - информацию о проверяемых файлах и URL-адресах: контрольные суммы проверяемого файла (MD5, SHA2-256, SHA1) и паттернов файла (MD5), размер паттерна, тип обнаруженной угрозы и её название согласно классификации Правообладателя, идентификатор антивирусных баз, URL-адрес, по которому запрашивается репутация, а также URL-адрес страницы, с которой осуществлён переход на проверяемый URL-адрес, идентификатор протокола соединения и номер используемого
  - порта; идентификатор задачи проверки, при выполнении которой обнаружена угроза;
  - информацию об используемых цифровых сертификатах, необходимую для проверки их подлинности:
    контрольные суммы (SHA256) сертификата, которым подписан проверяемый объект, и

    открытого ключа сертификата; идентификатор компонента ПО, выполняющего проверку;
  - идентификаторы антивирусных баз и записей в антивирусных базах;
  -
  - информацию о ПО Правообладателя: тип и полная версия программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, версия используемого протокола соединения с сервисами "Лаборатории Касперского";

- информацию об активации ПО на Компьютере: подписанный заголовок тикета от службы активации (идентификатор регионального центра активации, контрольную сумму кода активации, контрольную сумму тикета, дату создания тикета, уникальный идентификатор тикета, версию тикета, статус лицензии, дату и время начала / окончания действия тикета, уникальный идентификатор лицензии, версию лицензии), идентификатор сертификата, которым подписан заголовок тикета, контрольную сумму (MD5) файла ключа.

- Если в дополнение к флажку Kaspersky Security Network установлен флажок Включить расширенный режим KSN, программа дополнительно к перечисленному выше передает следующую информацию:

  - информацию о результатах категоризации запрашиваемых веб-ресурсов, которая содержит проверяемый URL-адрес и IP-адрес хоста, версию компонента ПО, выполнившего категоризацию, способ категоризации и набор категорий, определенных для веб-ресурса;

  - информацию об установленном на Компьютере программном обеспечении: название программного обеспечения и его производителей, используемые ключи реестра и их значения, информацию о файлах компонентов установленного программного обеспечения (контрольные суммы (MD5, SHA2-256, SHA1), имя, путь к файлу на Компьютере, размер, версию и цифровую подпись);

  - информацию о состоянии антивирусной защиты Компьютера: версии, даты и время выпуска используемых антивирусных баз, идентификатор задачи, выполняющего сканирование;

  - информацию о загружаемых Пользователем файлах: URL- и IP-адреса, откуда была выполнена загрузка, и URL-адрес страницы, с которой был выполнен переход на страницу загрузки файла, идентификатор протокола загрузки и номер порта соединения, признак вредоносности адресов, атрибуты и размер файла и его контрольные суммы (MD5, SHA2-256, SHA1), информацию о процессе, загрузившем файл (контрольные суммы (MD5, SHA2-256, SHA1), дата и время создания и линковки, признак нахождения в автозапуске, атрибуты, имена упаковщиков, информация о подписи, признак исполняемого файла, идентификатор формата, тип учетной записи, от имени которой был запущен процесс), информацию о файле процесса (имя, путь к файлу и размер), имя файла, путь к файлу на Компьютере, цифровая подпись файла и информация о выполнении подписи, URL-адрес, на котором произошло обнаружение, номер скрипта на странице, оказавшегося подозрительным или вредоносным;

  - информацию о запускаемых программах и их модулях: данные о запущенных процессах в системе (идентификатор процесса в системе (PID), имя процесса, данные об учетной записи, от которой запущен процесс, программе и команде, запустившей процесс, а также признак доверенности программы или процесса, полный путь к файлам процесса и их контрольные суммы (MD5, SHA2-256, SHA1), командная строка запуска, уровень целостности процесса, описание продукта, к которому относится процесс (название продукта и данные об издателе), а также данные об используемых цифровых сертификатах и информацию, необходимую для проверки их подлинности, или данные об отсутствии цифровой подписи файла), также информацию о загружаемых в процессы модулях (имя, размер, тип, дата создания, атрибуты, контрольные суммы (MD5, SHA2-256, SHA1), путь), информация заголовка PE-файлов, названия упаковщика (если файл был упакован);

  - информацию обо всех потенциально вредоносных объектах и действиях: название детектируемого объекта и полный путь к объекту на Компьютере, контрольные суммы обрабатываемых файлов (MD5, SHA2-256, SHA1), дата и время обнаружения, названия и размер обрабатываемых файлов и пути к ним, код шаблона пути, признак исполняемого файла, признак, является ли объект контейнером, названия упаковщика (если файл был упакован), код типа файла, идентификатор формата файла, идентификаторы антивирусных баз и записей в антивирусных базах, на основании которых было вынесено решение ПО, признак потенциально вредоносного объекта, название обнаруженной угрозы согласно классификации Правообладателя, степень опасности, статус и способ обнаружения, причина включения в анализируемый контекст и порядковый номер файла в контексте, контрольные суммы (MD5, SHA2-256, SHA1), имя и атрибуты исполняемого файла приложения, через которое прошло зараженное сообщение или ссылка, IP-адреса (IPv4 и IPv6)

хоста заблокированного объекта, энтропия файла, признак нахождения файла в автозапуске, время первого обнаружения файла в системе, количество запусков файла с момента последней отправки статистик, тип компилятора, информация о названии, контрольных суммах (MD5, SHA2-256, SHA1) и размере почтового клиента, через который был получен вредоносный объект, идентификатор задачи ПО, которое выполнило проверку, признак проверки репутации или подписи файла, результаты статического анализа содержимого объекта, паттерны объекта, размер паттерна в байтах, технические характеристики по применяемым технологиям детектирования;

- информацию о проверенных объектах: присвоенную группу доверия, в которую помещен и/или из которой перемещен файл, причина, по которой файл помещен в данную категорию, идентификатор категории, информация об источнике категорий и версии базы категорий, признак наличия у файла доверенного сертификата, название производителя файла, версия файла, имя и версия приложения, частью которого является файл;

- информацию об обнаруженных уязвимостях: идентификатор уязвимости в базе уязвимостей, класс опасности уязвимости;

- информацию о выполнении эмуляции исполняемого файла: размер файла и его контрольные суммы (MD5, SHA2-256, SHA1), версия компонента эмуляции, глубина эмуляции, вектор характеристик логических блоков и функций внутри логических блоков, полученный в ходе эмуляции, данные из структуры PE-заголовка исполняемого файла;

- информацию о сетевых атаках: IP-адреса атакующего компьютера (IPv4 и IPv6), номер порта Компьютера, на который была направлена сетевая атака, идентификатор протокола IP-пакета, в котором зафиксирована атака, цель атаки (название организации, веб-сайт), флаг реакции на атаку, весовой уровень атаки, значение уровня доверия;

- информацию об атаках, связанных с подменой сетевых ресурсов, DNS- и IP-адреса (IPv4 или IPv6) посещаемых веб-сайтов;

- DNS- и IP-адреса (IPv4 или IPv6) запрашиваемого веб-ресурса, информацию о файле и веб-клиенте, обращающемся к веб-ресурсу: название, размер, контрольные суммы (MD5, SHA2-256, SHA1) файла, полный путь к нему и код шаблона пути, результат проверки его цифровой подписи и его статус в KSN;

- информацию о выполнении отката деятельности вредоносной программы: данные о файле, активность которого откатывается (имя файла, полный путь к нему, его размер и контрольные суммы (MD5, SHA2-
256, SHA1)), данные об успешных и неуспешных действиях по удалению, переименованию и копированию файлов и восстановлению значений в реестре (имена ключей реестра и их значения), информация о системных файлах, изменённых вредоносной программой, до и после выполнения отката;

- информацию об исключениях для правил компонента Адаптивный контроль аномалий: идентификатор и статус сработавшего правила, действие ПО при срабатывании правила, тип учетной записи, от имени которой процесс или поток выполняет подозрительные действия, информацию о процессе, выполнившем подозрительные действия, и о процессе, в отношении которого были выполнены подозрительные действия (идентификатор скрипта или имя файла процесса, полный путь к файлу процесса, код шаблона пути, контрольные суммы (MD5, SHA2-256, SHA1) файла процесса), информацию об объекте, от имени которого были выполнены подозрительные действия, и об объекте, в отношении которого были выполнены подозрительные действия (название ключа реестра или имя файла, полный путь к файлу, код шаблона пути и контрольные суммы (MD5, SHA2-256, SHA1) файла);

- информацию о загружаемых ПО модулях: название, размер и контрольные суммы (MD5, SHA2-256, SHA1) файла модуля, полный путь к нему и код шаблона пути, параметры цифровой подписи файла модуля, дата и время создания подписи, название субъекта и организации, подписавших файл модуля, идентификатор процесса, в который был загружен модуль, название поставщика модуля, порядковый номер модуля в очереди загрузки;

- информацию о качестве работы ПО с сервисами KSN: дату и время начала и окончания периода формирования статистики, информацию о качестве запросов и соединения с каждым из используемых сервисов KSN (идентификатор сервиса KSN, количество успешных запросов, количество запросов с ответами из кеша, количество неуспешных запросов (сетевые проблемы, выключен KSN в параметрах ПО, неправильная маршрутизация), распределение по времени успешных запросов, распределение по времени отмененных запросов, распределение по времени запросов, превысивших ограничение на время ожидания, количество подключений к KSN, взятых из кеша, количество успешных подключений к KSN, количество неуспешных подключений к KSN, количество успешных транзакций, количество неуспешных транзакций, распределение по времени успешных подключений к KSN, распределение по времени неуспешных подключений к KSN, распределение по времени успешных транзакций, распределение по времени неуспешных транзакций);

- в случае обнаружения потенциально вредоносного объекта предоставляется информация о данных в памяти процессов: элементы иерархии системных объектов (ObjectManager), данные памяти UEFI BIOS, названия ключей реестра и их значения;

- информацию о событиях в системных журналах: время события, название журнала, в котором обнаружено событие, тип и категория события, название источника события и его описание;

- информацию о сетевых соединениях: версия и контрольные суммы (MD5, SHA2-256, SHA1) файла процесса, открывшего порт, путь к файлу процесса и его цифровая подпись, локальный и удалённый IPадреса, номера локального и удалённого портов соединения, состояние соединения, время открытия порта;

- информацию о дате установки и активации ПО на Компьютере: идентификатор партнера, у которого приобретена лицензия, серийный номер лицензии, уникальный идентификатор установки ПО на Компьютере, тип и идентификатор приложения, с которым выполняется обновление, идентификатор задачи обновления, информацию об установленных компонентах ПО и статус их работы;

- информацию о наборе всех установленных обновлений, а также о наборе последних установленных и/ или удалённых обновлений, тип события, служащего причиной отправки информации об обновлениях, период времени, прошедший после установки последнего обновления, информацию о загруженных в момент предоставления информации антивирусных базах;

- информацию о работе ПО на Компьютере: данные по использованию процессора (CPU), данные по использованию памяти (Private Bytes, Non-Paged Pool, Paged Pool), количество активных потоков в процессе ПО и потоков в состоянии ожидания, длительность работы ПО до возникновения ошибки, признак работы ПО в интерактивном режиме;

- количество дампов ПО и дампов системы (BSOD) с момента установки ПО и с момента последнего обновления, идентификатор и версия модуля ПО, в котором произошел сбой, стек памяти в продуктовом процессе и информация об антивирусных базах в момент сбоя;

- данные о дампе системы (BSOD): признак возникновения BSOD на Компьютере, имя драйвера, вызвавшего BSOD, адрес и стек памяти в драйвере, признак длительности сессии ОС до возникновения BSOD, стек памяти падения драйвера, тип сохраненного дампа памяти, признак того, что сессия работы ОС до BSOD длилась более 10 минут, уникальный идентификатор дампа, дата и время возникновения BSOD;

- данные об ошибках или проблемах с производительностью, возникших в работе компонентов ПО: идентификатор состояния ПО, тип, код и причина ошибки, а также время её возникновения, идентификаторы компонента, модуля и процесса продукта, в котором возникла ошибка, идентификатор задачи или категории обновления, при выполнении которой возникла ошибка, логи драйверов, используемых ПО (код ошибки, имя модуля, имя исходного файла и строка, где произошла ошибка);

- данные об обновлениях антивирусных баз и компонент ПО: имена, даты и время индексных файлов, загруженных в результате последнего обновления и загружаемых в текущем обновлении; • информацию об аварийных завершениях работы ПО: дату и время создания дампа, его тип, тип события, вызвавшего аварийное завершение работы ПО (непредвиденное отключение питания, падение приложения стороннего правообладателя), дату и время непредвиденного отключения питания;

- информацию о совместимости драйверов ПО с аппаратным и программным обеспечением: информацию о свойствах ОС, накладывающих ограничения на функциональность компонентов ПО (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), тип встроенного ПО загрузки (UEFI, BIOS), признак наличия доверенного платформенного модуля (Trusted Platform Module, TPM), версия спецификации TPM, информацию об установленном на компьютере центральном процессоре (CPU), режим и параметры работы Code Integrity и Device Guard, режим работы драйверов и причина использования текущего режима, версию драйверов ПО, статус поддержки драйверами программных и аппаратных средств виртуализации Компьютера;

- информацию о сторонних приложениях, вызвавших ошибку: их название, версию и локализацию, код ошибки и информацию о ней из системного журнала приложений, адрес возникновения ошибки и стек памяти стороннего приложения, признак возникновения ошибки в компоненте ПО, длительность работы стороннего приложения до возникновения ошибки, контрольные суммы (MD5, SHA2-256, SHA1) образа процесса приложения, в котором произошла ошибка, путь к этому образу процесса приложения и код шаблона пути, информацию из системного журнала ОС с описанием ошибки, связанной с приложением, информацию о модуле приложения, в котором произошла ошибка (идентификатор ошибки, адрес ошибки как смещение в модуле, имя и версию модуля, идентификатор падения приложения в плагине Правообладателя и стек памяти такого падения, время работы приложения до сбоя);

- версию компонента обновления ПО, количество аварийных завершений работы компонента обновления ПО при выполнении задач обновления за время работы компонента, идентификатор типа задачи обновления, количество неуспешных завершений задач обновления компонента обновления ПО;

- информацию о работе компонентов мониторинга системы: полные версии компонентов, дату и время запуска компонентов, код события, которое переполнило очередь событий, и количество таких событий, общее количество переполнений очереди событий, информация о файле процессаинициатора события (название файла и путь к нему на Компьютере, код шаблона пути, контрольные суммы (MD5, SHA2-256, SHA1) процесса, связанного с файлом, версия файла), идентификатор выполненного перехвата события, полная версия фильтра перехвата, идентификатор типа перехваченного события, размер очереди событий и количество событий между первым событием в очереди и текущим событием, количество просроченных событий в очереди, информация о процессеинициаторе текущего события (название файла процесса и путь к нему на Компьютере, код шаблона пути, контрольные суммы (MD5, SHA2-256, SHA1) процесса), время обработки события, максимально допустимое время обработки событий, значение вероятности отправки данных, информацию о событиях ОС, время обработки которых ПО превысило ограничение на время ожидания (дата и время получения события, количество повторных инициализаций антивирусных баз, дату и время последней повторной инициализации антивирусных баз после их обновления, время задержки обработки события каждым компонентом мониторинга системы, количество ожидающих событий, количество обработанных событий, количество

задержанных событий текущего типа, суммарное время задержки событий текущего типа, суммарное время задержки всех событий);

- информацию от инструмента трассировки событий Windows (Event Tracing for Windows, ETW) при проблемах с производительностью ПО, поставщики событий SysCon g / SysCon gEx / WinSATAssessment от Microsoft: данные о компьютере (модель, производитель, форм-фактор корпуса, версия), данные о метриках производительности Windows (данные WinSAT-оценки, индекс производительности Windows), имя домена, данные о физических и логических процессорах (количество физических и логических процессоров, производитель, модель, степпинг, количество ядер, тактовая частота, идентификатор процессора (CPUID), характеристики кэша, характеристики логического процессора, признаки поддержки режимов и инструкций), данные о модулях оперативной памяти (тип, форм-фактор, производитель, модель, объем, гранулярность выделения памяти), данные о сетевых интерфейсах (IP- и MAC-адреса, название, описание, конфигурация сетевых интерфейсов, распределение числа и объема сетевых пакетов по типам, скорость сетевого обмена, распределение числа сетевых ошибок по типам), конфигурацию IDE-контроллера, IP-адреса DNS-серверов, данные о видеокарте (модель, описание, производитель, совместимость, объем видеопамяти, разрешение экрана, количество бит на пиксель, версия BIOS), данные о подключенных самонастраиваемых (Plugand-Play) устройствах (название, описание, идентификатор устройства [PnP, ACPI], данные о дисках и накопителях (количество дисков или флеш-накопителей, производитель, модель, объем диска, число цилиндров, число дорожек на цилиндр, число секторов на дорожку, объем сектора, характеристики кэша, порядковый номер, число разделов, конфигурация контролера SCSI), данные о логических дисках (порядковый номер, объем раздела, объем тома, буква тома, тип раздела, тип файловой системы, количество кластеров, размер кластера, число секторов в кластере, число занятых и свободных кластеров, буква загрузочного тома, адрес-смещение раздела относительно начала диска), данные о BIOS материнской платы (производитель, дата выпуска, версия), данные о материнской плате (производитель, модель, тип), данные о физической памяти (общий и свободный объем), данные о службах операционной системы (имя, описание, статус, тег, данные о процессах [имя и идентификатор PID]), параметры энергопотребления компьютера, конфигурацию контролера прерываний, пути к системным папкам Windows (Windows и System32), данные об ОС (версия, сборка, дата выпуска, название, тип, дата установки), размер файла подкачки, данные о мониторах (количество, производитель, разрешение экрана, разрешающая способность, тип), данные о драйвере видеокарты (производитель, дата выпуска, версия);

- информацию от ETW, поставщики событий EventTrace / EventMetadata от Microsoft: данные о последовательности системных событий (тип, время, дата, часовой пояс), метаданные о файле с результатами трассировки (имя, структура, параметры трассировки, распределение числа операций трассировки по типам), данные об ОС (название, тип, версия, сборка, дата выпуска, время старта);

- информацию от ETW, поставщики событий Process / Microsoft-Windows-Kernel-Process / MicrosoftWindows-Kernel-Processor-Power от Microsoft: данные о запускаемых и завершаемых процессах (имя, идентификатор PID, параметры старта, командная строка, код возврата, параметры управления питанием, время запуска и завершения, тип маркера доступа, идентификатор безопасности SID, идентификатор сеанса SessionID, число установленных дескрипторов), данные об изменении приоритетов потоков (идентификатор потока TID, приоритет, время), данные о дисковых операциях процесса (тип, время, объем, число), история изменения структуры и объема используемой процессом памяти;

- информацию от ETW, поставщики событий StackWalk / Per nfo от Microsoft: данные счетчиков производительности (производительность отдельных участков кода, последовательность вызовов функций, идентификатор процесса PID, идентификатор потока TID, адреса и атрибуты обработчиков прерываний ISR и отложенных вызовов процедур DPC);

- информацию от ETW, поставщик событий KernelTraceControl-ImageID от Microsoft: данные об исполняемых файлах и динамических библиотеках (имя, размер образа, полный путь), данные о PDBфайлах (имя, идентификатор), данные ресурса VERSIONINFO исполняемого файла (название, описание, производитель, локализация, версия и идентификатор приложения, версия и идентификатор файла);

- информацию от ETW, поставщики событий FileIo / DiskIo / Image / Windows-Kernel-Disk от Microsoft: данные о файловых и дисковых операциях (тип, объем, время начала, время завершения, длительность, статус завершения, идентификатор процесса PID, идентификатор потока TID, адреса вызовов функций драйвера, пакет запроса ввода-вывода (I/O Request Packet, IRP), атрибуты файлового объекта Windows), данные о файлах, участвующих в файловых и дисковых операциях (имя, версия, размер, полный путь, атрибуты, смещение, контрольная сумма образа, опции открытия и доступа);

- информацию от ETW, поставщик событий PageFault от Microsoft: данные об ошибках доступа к страницам памяти (адрес, время, объем, идентификатор процесса PID, идентификатор потока TID, атрибуты файлового объекта Windows, параметры выделения памяти);

- информацию от ETW, поставщик событий Thread от Microsoft: данные о создании / завершении потоков, данные о запущенных потоках (идентификатор процесса PID, идентификатор потока TID, размер стека, приоритеты и распределение ресурсов CPU, ресурсов ввода-вывода, страниц памяти между потоками, адрес стека, адрес начальной функции, адрес блока окружения потока (Thread Environment Block, TEB), тег службы Windows);

- информацию от ETW, поставщик событий Microsoft-Windows-Kernel-Memory от Microsoft: данные об операциях управления памятью (статус завершения, время, количество, идентификатор процесса PID), структура распределения памяти (тип, объем, идентификатор сеанса SessionID, идентификатор процесса PID);

- информацию о работе ПО при появлении проблем с производительностью: идентификатор установки ПО, тип и значение снижения производительности, данные о последовательности внутренних событий ПО (время, часовой пояс, тип, статус завершения, идентификатор компонента ПО, идентификатор сценария работы ПО, идентификатор потока TID, идентификатор процесса PID, адреса вызовов функций), данные о проверяемых сетевых соединениях (URL, направление соединения, размер сетевого пакета), данные о PDB-файлах (имя, идентификатор, размер образа исполняемого файла), данные о проверяемых файлах (имя, полный путь, контрольная сумма), параметры мониторинга производительности ПО;

- информацию о неуспешной последней перезагрузке ОС: количество неуспешных перезагрузок с момента установки ОС, данные о дампе системы (код и параметры ошибки, имя, версия и контрольная сумма (CRC32) модуля, вызвавшего ошибку в работе ОС, адрес ошибки как смещение в модуле, контрольные суммы (MD5, SHA2-256, SHA1) дампа системы);

- информацию для проверки подлинности сертификатов, которыми подписаны файлы: отпечаток сертификата, алгоритм вычисления контрольной суммы, публичный ключ и серийный номер сертификата, имя эмитента сертификата, результат проверки сертификата и идентификатор базы сертификатов;

- информацию о процессе, выполняющем атаку на самозащиту ПО: имя и размер файла процесса, его контрольные суммы (MD5, SHA2-256, SHA1), полный путь к нему и код шаблона пути, даты и время создания и компоновки файла процесса, код типа файла процесса, признак исполняемого файла, атрибуты файла процесса, информацию о сертификате, которым подписан файл процесса, тип учетной записи, от имени которой процесс или поток выполняет подозрительные действия, идентификатор операций, которые осуществлялись для доступа к процессу, тип ресурса, с которым выполняется операция (процесс, файл, объект реестра, поиск окна с помощью функции

FindWindow), имя ресурса, с которым выполняется операция, признак успешности выполнения операции, статус файла процесса и его подписи в KSN;

- информацию о ПО Правообладателя: локализацию и статус работы используемого ПО, версии установленных компонентов ПО и статус их работы, данные об установленных обновлениях ПО, а также значение фильтра TARGET;

- информацию об установленном на Компьютере аппаратном обеспечении: тип, название, модель, версию прошивки, характеристики встроенных и подключенных устройств, уникальный идентификатор Компьютера, на котором установлено ПО;

- информацию о версии установленной на Компьютере операционной системы (ОС) и

установленных пакетов обновлений, разрядность, редакцию и параметры режима работы ОС,

- версию и контрольные суммы (MD5, SHA2-256, SHA1) файла ядра ОС, дату и время запуска ОС;
- исполняемые и неисполняемые файлы целиком или частично, в том числе доверенные файлы;
- участки оперативной памяти Компьютера; сектора, участвующие в процессе загрузки
- операционной системы; пакеты данных сетевого трафика; веб-страницы и электронные письма,
- содержащие подозрительные и вредоносные объекты; описание классов и экземпляров классов
- WMI хранилища;
-

- отчеты об активностях приложений: имя, размер и версия отправляемого файла, его описание и контрольные суммы (MD5, SHA2-256, SHA1), идентификатор формата, название его производителя, название продукта, к которому относится файл, полный путь к файлу на Компьютере и код шаблона пути, дата и время создания и модификации файла; даты и время начала и окончания срока действия сертификата, если отправляемый файл имеет ЭЦП, дата и время подписания, имя эмитента сертификата, информация о владельце сертификата, отпечаток и открытый ключ сертификата и алгоритмы их вычисления, серийный номер сертификата; имя учетной записи, от которой запущен процесс; контрольные суммы (MD5, SHA2-256, SHA1) имени Компьютера, на котором запущен процесс; заголовки окон процесса; идентификатор антивирусных баз, название обнаруженной угрозы согласно классификации Правообладателя; информацию об установленной в ПО лицензии, идентификатор лицензии, ее тип и дата истечения; локальное время Компьютера в момент предоставления информации; имена и пути к файлам, к которым получал доступ процесс; имена ключей реестра и их значения, к которым получал доступ процесс; URL- и IP-адреса, к которым обращался процесс; URL- и IP-адреса, с которых был получен запускаемый файл.

Включение и выключение использования Kaspersky Security Network

Чтобы включить или выключить использование Kaspersky Security Network, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Продвинутая защита → Kaspersky Security Network.

3. Установите флажок Kaspersky Security Network, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использовал информацию о репутации файлов, веб-ресурсов и программ, полученную из Kaspersky Security Network.

   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready покажет Положение о Kaspersky Security Network. Если вы согласны, примите условия использования KSN.

   По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует расширенный режим KSN. Расширенный режим KSN – режим работы программы, при котором Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready передает в "Лабораторию Касперского" дополнительные данные.

4. Если требуется, снимите флажок Включить расширенный режим KSN.

5. Сохраните внесенные изменения.

Включение и выключение облачного режима для компонентов защиты

При использовании Kaspersky Private Security Network функциональность облачного режима доступна начиная с версии Kaspersky Private Security Network 3.0.

Чтобы включить или выключить облачный режим для компонентов защиты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Продвинутая защита → Kaspersky Security Network.

3. Выполните одно из следующих действий:

   - Установите флажок Включить облачный режим для компонентов защиты.

     Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует облегченную версию антивирусных баз, за счет чего снижается нагрузка на ресурсы операционной системы.

     Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready загружает облегченную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был установлен.

     Если облегченная версия антивирусных баз недоступна для использования, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически переключается на использование полной версии антивирусных баз.

   - Снимите флажок Включить облачный режим для компонентов защиты.

     Если флажок снят, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует полную версию антивирусных баз.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready загружает полную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был снят.

Флажок доступен, если установлен флажок Kaspersky Security Network.

4. Сохраните внесенные изменения.

Проверка подключения к Kaspersky Security Network

Чтобы проверить подключение к Kaspersky Security Network, выполните следующие действия:

1. В главном окне программы нажмите на блок Технологии обнаружения угроз.

   В нижней части окна Технологии обнаружения угроз отображается следующая информация о работе Kaspersky Security Network:

   - Под строкой Kaspersky Security Network (KSN) отображается один из следующих статусов подключения Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready к Kaspersky Security Network:

     - Включено. Доступно.

       Статус означает, что Kaspersky Security Network используется в работе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и серверы KSN доступны.

     - Включено. Недоступно.

       Статус означает, что Kaspersky Security Network используется в работе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и серверы KSN недоступны.

     - Отключено.

       Статус означает, что Kaspersky Security Network не используется в работе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

   - В строках Безопасных объектов, Опасных объектов, Нейтрализованных угроз за сутки отображается глобальная статистика инфраструктуры облачных служб Kaspersky Security Network.

   - В строке Последняя синхронизация отображается дата и время последней синхронизации Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready с серверами KSN.

     Получение статистических данных по использованию KSN программа производит при открытии окна Технологии обнаружения угроз. Обновление глобальной статистики инфраструктуры облачных служб Kaspersky Security Network, а также строки Последняя синхронизация в реальном времени не производится.

     Если время, прошедшее после последней синхронизации с серверами KSN, превышает 15 минут или отображается статус Неизвестно, то статус подключения Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready к Kaspersky Security Network принимает значение Включено. Недоступно.

Связь с серверами Kaspersky Security Network может отсутствовать по следующим причинам:

- Ваш компьютер не подключен к интернету.
- Программа не активирована.
- Срок действия лицензии истек.
- Выявлены проблемы, связанные с лицензионным ключом (например, ключ попал в черный список ключей).

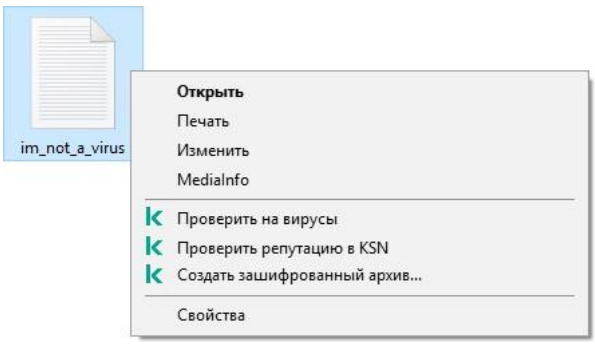
Если восстановить связь с серверами Kaspersky Security Network не удается, то рекомендуется обратиться в Службу технической поддержки или к поставщику услуг.

Проверка репутации файла в Kaspersky Security Network

Если вы сомневаетесь в безопасности файла, вы можете проверить его репутацию в Kaspersky Security Network.

Проверка репутации файла доступна, если вы приняли условия Положения о Kaspersky Security Network.

Чтобы проверить репутацию файла в Kaspersky Security Network, откройте контекстное меню файла и выберите пункт Проверить репутацию в KSN (см. рис. ниже).



Контекстное меню файла

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображает репутацию файла:

Доверенный. Большинство пользователей Kaspersky Security Network подтвердили, что файл доверенный.

Легальная программа, которая может быть использована для нанесения вреда компьютеру или данным. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы

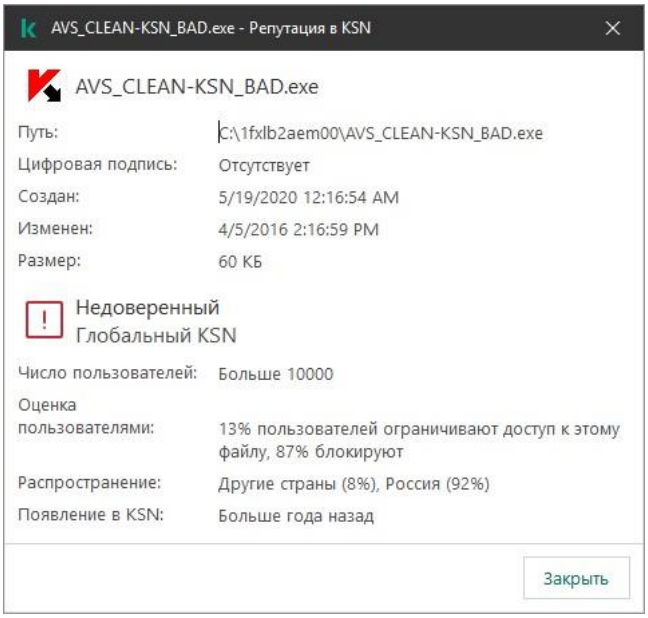
можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского". Вы можете добавить эти программы в список доверенных.

Недоверенный. Вирус или другая программа, представляющая угрозу.

Неизвестный. В Kaspersky Security Network отсутствует информация о файле. Вы можете проверить файл с помощью антивирусных баз (пункт контекстного меню Проверить на вирусы).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображает решение KSN, которое было использовано для определения репутации файла: Глобальный KSN или Локальный KSN.

Также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображает дополнительную информацию о файле (см. рис. ниже).



Репутация файла в Kaspersky Security Network

Анализ поведения

Компонент Анализ поведения получает данные о действиях программ на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы.

Компонент Анализ поведения использует шаблоны опасного поведения программ. Если активность программы совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

Включение и выключение Анализа поведения

По умолчанию Анализ поведения включен и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". Вы можете выключить Анализ поведения при необходимости.

Не рекомендуется выключать Анализ поведения без необходимости, так как это снижает эффективность работы компонентов защиты. Компоненты защиты могут запрашивать данные, полученные компонентом Анализ поведения, для обнаружения угроз.

Чтобы включить или выключить Анализ поведения, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Анализ поведения.
3. Выполните одно из следующих действий:
   - Установите флажок Анализ поведения, если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready анализировал активность программ в операционной системе, используя шаблоны опасного поведения.
   - Снимите флажок Анализ поведения, если вы не хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready анализировал активность программ в операционной системе, используя шаблоны опасного поведения.
4. Сохраните внесенные изменения.

Выбор действия при обнаружении вредоносной активности программы

Чтобы выбрать действие при обнаружении вредоносной активности программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Анализ поведения.
3. В раскрывающемся списке При обнаружении вредоносной активности программы выберите нужное действие:
   - Удалять файл.

     Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет исполняемый файл вредоносной программы и создает резервную копию файла в резервном хранилище.
   - Завершать работу программы.

     Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready завершает работу этой программы.
   - Информировать.

     Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security добавляет информацию о вредоносной активности этой программы в список активных угроз.

4. Сохраните внесенные изменения.

Защита папок общего доступа от внешнего шифрования

Компонент обеспечивает отслеживание операций только над теми файлами, которые расположены на запоминающих устройствах с файловой системой NTFS и не зашифрованы системой EFS.

Функция защиты папок общего доступа от внешнего шифрования обеспечивает анализ активности в папках общего доступа. Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready выполняет выбранное действие.

По умолчанию защита папок общего доступа от внешнего шифрования выключена.

После установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

Включение и выключение защиты папок общего доступа от внешнего шифрования

После установки Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

Чтобы включить или выключить защиту папок общего доступа от внешнего шифрования, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Анализ поведения.
3. В блоке Защита папок общего доступа от внешнего шифрования выполните одно из следующих действий:
   - Установите флажок Включить защиту папок общего доступа от внешнего шифрования, если вы хотите, чтобы программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready анализировала активность, характерную для внешнего шифрования.
   - Снимите флажок Включить защиту папок общего доступа от внешнего шифрования, если вы не хотите, чтобы программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready анализировала активность, характерную для внешнего шифрования.
4. Сохраните внесенные изменения.

Выбор действия при обнаружении внешнего шифрования папок общего доступа

Чтобы выбрать действие при обнаружении внешнего шифрования папок общего доступа, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Анализ поведения.
3. В блоке Защита папок общего доступа от внешнего шифрования в раскрывающемся списке При обнаружении внешнего шифрования папок общего доступа выберите нужное действие:
   - Блокировать соединение.

     Если выбран этот вариант, то при обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready выполняет следующие действия: блокирует сетевую активность компьютера, осуществляющего изменение; создает резервные копии подверженных изменению файлов; добавляет запись в отчеты локального интерфейса программы; отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

     Если при этом включен компонент Откат вредоносных действий, то выполняется восстановление измененных файлов из резервных копий.

     Если вы выбрали элемент Блокировать соединение, то вы можете указать время в минутах, на которое будет заблокировано сетевое соединение, в поле Блокировать соединение на N минут.
   - Информировать.

     Если выбран этот вариант, то при обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready добавляет запись в отчеты локального интерфейса программы, добавляет запись в список активных угроз и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.
4. Сохраните внесенные изменения.

Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования

Для работы функциональности исключений адресов из защиты папок общего доступа от внешнего шифрования необходимо включить службу Аудит входа в систему. По умолчанию служба Аудит входа в систему выключена (подробную информацию о включении службы Аудит входа в систему см. на сайте корпорации Microsoft).

Функциональность исключений адресов из защиты папок общего доступа не работает на удаленном компьютере, если этот удаленный компьютер был включен до запуска Kaspersky Endpoint Security для

бизнеса - Расширенный EDR Ready. Вы можете перезагрузить этот удаленный компьютер после запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, чтобы обеспечить работу функциональности исключений адресов из защиты папок общего доступа на этом удаленном компьютере.

Чтобы исключить из защиты удаленные компьютеры, осуществляющие внешнее шифрование папок общего доступа, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Анализ поведения.
3. В блоке Защита папок общего доступа от внешнего шифрования нажмите на кнопку Исключения.

   Откроется окно Исключения.
4. Выполните одно из следующих действий:

   - Если вы хотите добавить IP-адрес или имя компьютера в список исключений, нажмите на кнопку Добавить.
   - Если вы хотите изменить IP-адрес или имя компьютера, выберите его в списке исключений и нажмите на кнопку Изменить.

   Откроется окно Компьютер.
5. Введите IP-адрес компьютера или имя компьютера, попытки внешнего шифрования с которого не должны обрабатываться.
6. Сохраните внесенные изменения.

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимую программу. При обработке этих данных уязвимая программа выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО.

Если попытка запустить исполняемый файл из уязвимой программы не была произведена пользователем, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует запуск этого файла или информирует пользователя.

Включение и выключение Защиты от эксплойтов

По умолчанию Защита от эксплойтов включена и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". Вы можете выключить Защиту от эксплойтов при необходимости.

Чтобы включить или выключить Защиту от эксплойтов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Защита от эксплойтов.
3. Выполните одно из следующих действий:
   - Установите флажок Защита от эксплойтов, если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отслеживал исполняемые файлы, запускаемые уязвимыми программами.

     Если Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обнаруживает, что исполняемый файл из уязвимой программы был запущен не пользователем, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет действие, выбранное в раскрывающемся списке При обнаружении эксплойта.
   - Снимите флажок Защита от эксплойтов, если вы не хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отслеживал исполняемые файлы, запускаемые уязвимыми программами.
4. Сохраните внесенные изменения.

Выбор действия при обнаружении эксплойта

По умолчанию, обнаружив эксплойт, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует операции этого эксплойта.

Чтобы выбрать действие при обнаружении эксплойта, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Защита от эксплойтов.
3. В раскрывающемся списке При обнаружении эксплойта выберите нужное действие:
   - Блокировать операцию.

     Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте.
   - Информировать.

     Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз.
4. Сохраните внесенные изменения.

Включение и выключение защиты памяти системных процессов

По умолчанию защита памяти системных процессов включена.

Чтобы включить или выключить защиту памяти системных процессов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Защита от эксплойтов.
3. Выполните одно из следующих действий:
   - В блоке Защита памяти системных процессов установите флажок Включить защиту памяти системных процессов, если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокировал сторонние процессы, осуществляющие попытки доступа к системным процессам.
   - В блоке Защита памяти системных процессов снимите флажок Включить защиту памяти системных процессов, если вы не хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокировал сторонние процессы, осуществляющие попытки доступа к системным процессам.
4. Сохраните внесенные изменения.

Предотвращение вторжений

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Предотвращение вторжений (англ. HIPS – Host Intrusion Prevention System) предотвращает выполнение программами опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным. Компонент обеспечивает защиту компьютера с помощью антивирусных баз и облачной службы Kaspersky Security Network.

Компонент контролирует работу программ с помощью прав программ. Права программ включают в себя следующие параметры доступа:

- доступ к ресурсам операционной системы (например, параметры автозапуска, ключи реестра);
- доступ к персональным данным (например, к файлам, программам).

Сетевую активность программ контролирует Сетевой экран с помощью сетевых правил.

Во время первого запуска программы компонент Предотвращение вторжений выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.

2. Проверяет безопасность программы в Kaspersky Security Network.

   Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает программу в одну из групп доверия: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

   Группа доверия определяет права, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует для контроля сетевой активности программ. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready помещает программу в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

   Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready помещает программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует действия программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещен доступ к модулям операционной системы.

При следующем запуске программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие права программ. Если программа была изменена, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready исследует программу как при первом запуске.

Ограничения контроля аудио и видео устройств

О защите аудиосигнала

Функциональность защиты аудиосигнала имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Предотвращение вторжений.
-

Если программа начала получать аудиосигнал до запуска компонента Предотвращение вторжений, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает программе получение аудиосигнала и не показывает никаких уведомлений.

- Если вы поместили программу в группу Недоверенные или Сильные ограничения после того, как программа начала получать аудиосигнал, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает программе получение аудиосигнала и не показывает никаких уведомлений.

- При изменении параметров доступа программы к устройствам записи звука (например, программе было запрещено получение аудиосигнала в окне параметров Предотвращение вторжений) требуется перезапуск этой программы, чтобы она перестала получать аудиосигнал.

- Контроль получения аудиосигнала с устройств записи звука не зависит от параметров доступа программ к веб-камере.

- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready защищает доступ только к встроенным и внешним микрофонам. Другие устройства передачи звука не поддерживаются.

- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не гарантирует защиту аудиосигнала, передаваемого с таких устройств, как DSLR-камеры, портативные видеокамеры, экшн-камеры.

Особенности работы аудио и видео устройств во время установки и обновления Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready

При первом запуске программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с момента ее установки воспроизведение или запись аудио и видео могут быть прерваны в программах записи или воспроизведения аудио и видео. Это необходимо для того, чтобы включилась функциональность контроля доступа программ к устройствам записи звука. Системная служба управления средствами работы со звуком будет перезапущена при первом запуске программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

О доступе программ к веб-камерам

Функциональность защиты доступа к веб-камере имеет следующие особенности и ограничения:

- Программа контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.

- Программа контролирует аудиосигнал, если он является частью видеопотока, получаемого с веб-камеры.
-

Программа контролирует только веб-камеры, подключаемые по интерфейсу USB или IEEE1394 и отображаемые в Диспетчере устройств Windows как Устройства обработки изображений (Imaging Device).

Поддерживаемые веб-камеры

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает следующие веб-камеры:

- Logitech HD Webcam C270;
- Logitech HD Webcam C310;
- Logitech Webcam C210;
- Logitech Webcam Pro 9000;
- Logitech HD Webcam C525;
- Microsoft LifeCam VX-1000;
- Microsoft LifeCam VX-2000;
- Microsoft LifeCam VX-3000;
- Microsoft LifeCam VX-800;
- Microsoft LifeCam Cinema.

"Лаборатория Касперского" не гарантирует поддержку веб-камер, не указанных в этом списке.

Включение и выключение Предотвращения вторжений

По умолчанию компонент Предотвращение вторжений включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить компонент Предотвращение вторжений при необходимости.

Чтобы включить или выключить компонент Предотвращение вторжений выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.
3. В правой части окна выполните одно из следующих действий:
   - Установите флажок Предотвращение вторжений, если вы хотите включить компонент Предотвращение вторжений.
   - Снимите флажок Предотвращение вторжений, если вы хотите выключить компонент Предотвращение вторжений.
4. Сохраните внесенные изменения.

Работа с группами доверия программ

Во время первого запуска каждой программы компонент Предотвращение вторжений проверяет безопасность программы и помещает программу в одну из групп доверия.

На первом этапе проверки программы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready ищет запись о программе во внутренней базе известных программ и одновременно отправляет запрос в базу Kaspersky Security Network (при наличии подключения к интернету). По результатам проверки по внутренней базе и по базе Kaspersky Security Network программа помещается в группу доверия. При каждом повторном запуске программы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready отправляет новый запрос в базу KSN и перемещает программу в другую группу доверия, если репутация программы в базе KSN изменилась.

Вы можете выбрать группу доверия, в которую Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready должен автоматически помещать все неизвестные программы. Программы, которые были запущены до Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, автоматически помещаются в группу доверия, указанную в окне Выбор группы доверия.

Для программ, запущенных до Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, контролируется только сетевая активность.
Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана.

Настройка параметров распределения программ по группам доверия

Если участие в Kaspersky Security Network включено, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready отправляет запрос о репутации программы в KSN при каждом запуске программы. На основе полученного ответа программа может быть перемещена в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready всегда помещает программы, подписанные сертификатами Microsoft или сертификатами "Лаборатории Касперского", в группу доверия "Доверенные".

Чтобы настроить параметры распределения программ по группам доверия, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.
3. Если вы хотите автоматически помещать программы с цифровой подписью в группу доверия "Доверенные", установите флажок Доверять программам, имеющим цифровую подпись.
4. Чтобы помещать все неизвестные программы в указанную группу доверия, выберите нужную группу доверия из раскрывающегося списка Программы, для которых не удалось определить группу доверия, автоматически помещать в.

В целях безопасности группа Доверенные не включена в значения параметра Программы, для которых не удалось определить группу доверия, автоматически помещать в.

5. Сохраните внесенные изменения.

Изменение группы доверия

Во время первого запуска программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически помещает программу в ту или иную группу доверия. При необходимости вы можете вручную переместить программу в другую группу доверия.

Специалисты "Лаборатории Касперского" не рекомендуют перемещать программы из группы доверия, определенной автоматически, в другую группу доверия. Вместо этого при необходимости измените права отдельной программы.

Чтобы изменить группу доверия, в которую Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически поместил программу при первом ее запуске, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.
3. Нажмите на кнопку Программы.

   Откроется закладка Права программ окна Предотвращение вторжений.
4. На закладке Права программ выберите нужную программу.
5. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню программы. В контекстном меню программы выберите пункт Переместить в группу → <название группы>.
   - По ссылке Доверенные / Слабые ограничения / Сильные ограничения / Недоверенные откройте контекстное меню. В контекстном меню выберите нужную группу доверия.
6. Сохраните внесенные изменения.

Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready

Для программ, запущенных до Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, контролируется только сетевая активность.
Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана. Чтобы указать, какими сетевыми правилами должен регулироваться контроль сетевой активности таких программ, необходимо выбрать группу доверия.

Чтобы выбрать группу доверия для программ, запускаемых до Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.
3. Нажмите на кнопку Изменить.

   Откроется окно Выбор группы доверия.
4. Выберите нужную группу доверия.
5. Сохраните внесенные изменения.

Работа с правами программ

По умолчанию для контроля работы программы применяются права программ, определенные для той группы доверия, в которую Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поместил программу при первом ее запуске. При необходимости вы можете изменить права программ для всей группы доверия, для отдельной программы или группы программ внутри группы доверия.

Права программ, определенные для отдельных программ или групп программ внутри группы доверия, имеют более высокий приоритет, чем права программ, определенные для группы доверия. То есть, если параметры прав программ, определенные для отдельной программы или группы программ внутри группы доверия, отличны от параметров прав программ, определенных для группы доверия, то компонент Предотвращение вторжений контролирует работу программы или группы программ внутри группы доверия в соответствии с правами программ, определенными для программы или группы программ.

Изменение прав программ для групп доверия и для групп программ

По умолчанию для разных групп доверия созданы оптимальные права программ. Параметры прав групп программ, входящих в группу доверия, наследуют значения параметров прав групп доверия. Вы можете изменить предустановленные права групп доверия и права групп программ.

Чтобы изменить права группы доверия или права группы программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.
3. Нажмите на кнопку Программы.

   Откроется закладка Права программ окна Предотвращение вторжений.
4. Выберите нужную группу доверия или группу программ.
5. В контекстном меню группы доверия или группы программ выберите пункт Права группы.

   Откроется окно Права группы программ.
6. В окне Права группы программ выполните одно из следующих действий:

- Выберите закладку Файлы и системный реестр, если вы хотите изменить права группы доверия или права группы программ, регулирующие права группы доверия или группы программ на операции с реестром операционной системы, файлами пользователя и параметрами программ.

- Выберите закладку Права, если вы хотите изменить права группы доверия или права группы программ, регулирующие права группы доверия или группы программ на доступ к процессам и объектам операционной системы.

7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню.

8. В контекстном меню выберите нужный пункт:

   - Наследовать.
   - Разрешать.
   - Запрещать.
   - Записывать в отчет.

   Если вы изменяете правила контроля группы доверия, то пункт Наследовать недоступен для выбора.

9. Сохраните внесенные изменения.

Изменение прав программы

По умолчанию параметры прав программ, входящих в группу программ или в группу доверия, наследуют значения параметров прав группы доверия. Вы можете изменить параметры прав программ.

Чтобы изменить права программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.
3. Нажмите на кнопку Программы.

   Откроется закладка Права программ окна Предотвращение вторжений.
4. Выберите нужную программу.
5. Выполните одно из следующих действий:

   - В контекстном меню программы выберите пункт Права программы.
   - Нажмите на кнопку Дополнительно в правом нижнем углу закладки Права программ.

   Откроется окно Права программы.

6. В окне Права программы выполните одно из следующих действий:

   - Выберите закладку Файлы и системный реестр, если вы хотите изменить права программы, регулирующие права программы на операции с реестром операционной системы, файлами пользователя и параметрами программ.

   - Выберите закладку Права, если вы хотите изменить права программы, регулирующие права программы на доступ к процессам и объектам операционной системы.

7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню.

8. В контекстном меню выберите нужный пункт:

   - Наследовать.
   - Разрешать.
   - Запрещать.
   - Записывать в отчет.

9. Сохраните внесенные изменения.

Выключение загрузки и обновления прав программ из базы Kaspersky Security Network

По умолчанию при обнаружении в базе Kaspersky Security Network новой информации о программе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready применяет для этой программы права, загруженные из базы KSN. После этого вы можете изменить права программы вручную.

Если на момент первого своего запуска программа отсутствовала в базе Kaspersky Security Network, но затем информация о ней была добавлена в базу Kaspersky Security Network, то по умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически обновляет права этой программы.

Вы можете выключить загрузку прав программ из базы Kaspersky Security Network и автоматическое обновление прав ранее неизвестных программ.

Чтобы выключить загрузку и обновление прав программ из базы Kaspersky Security Network, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.

3. Снимите флажок Обновлять права для ранее неизвестных программ из базы KSN.

4. Сохраните внесенные изменения.

Выключение наследования ограничений родительского процесса

Инициатором запуска программы может быть как пользователь, так и другая запущенная программа. Если инициатором запуска программы является другая программа, образуется последовательность запуска, состоящая из родительских и дочерних процессов.

Когда программа пытается получить доступ к защищаемому ресурсу, компонент Предотвращение вторжений анализирует права всех родительских процессов этой программы на доступ к защищаемому ресурсу. При этом применяются права минимального приоритета: при сравнении прав доступа программы и родительского процесса к активности программы применяются права доступа с минимальным приоритетом.

Приоритет прав доступа следующий:

1. Разрешать. Это право доступа имеет высший приоритет.
2. Запрещать. Это право доступа имеет низший приоритет.

Этот механизм предотвращает использование доверенных программ недоверенными или ограниченными в правах программами с целью выполнения привилегированных действий.

Если действие программы блокируется по причине недостатка прав у одного из родительских процессов, вы можете изменить эти права или выключить наследование ограничений родительского процесса.

Чтобы выключить наследование ограничений родительского процесса, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.
3. Нажмите на кнопку Программы.

   Откроется закладка Права программ окна Предотвращение вторжений.
4. Выберите нужную программу.
5. В контекстном меню программы выберите пункт Права программы.

   Откроется окно Права программы.
6. В окне Права программы выберите закладку Исключения.
7. Установите флажок Не наследовать ограничения родительского процесса (программы).
8. Сохраните внесенные изменения.

Исключение некоторых действий программ из прав программ

Чтобы исключить некоторые действия программы из прав программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.

3. Нажмите на кнопку Программы.

   Откроется закладка Права программ окна Предотвращение вторжений.

4. Выберите нужную программу.

5. В контекстном меню программы выберите пункт Права программы.

   Откроется окно Права программы.

6. Выберите закладку Исключения.

7. Установите флажки напротив действий программы, которые не нужно контролировать.

8. Сохраните внесенные изменения.

Удаление информации о неиспользуемых программах

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует работу программ с помощью прав программ. Права программы определены группой доверия. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready помещает программу в группу доверия при первом запуске. Вы можете изменить группу доверия для программы вручную. Также вы можете настроить права для отдельной программы вручную. Таким образом, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready хранит следующую информацию о программе: группа доверия и права программы.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически удаляет информацию о неиспользуемых программах для экономии ресурсов компьютера. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет информацию о программах по следующим правилам:

- Если группа доверия и права программы определены автоматически, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет информацию об этой программе через 30 дней. Изменить время хранения информации о программе или выключить автоматическое удаление невозможно.

- Если вы вручную поместили программу в группу доверия или настроили права доступа, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет информацию об этой программе через 60 дней (значение по умолчанию). Вы можете изменить время хранения информации о программе или выключить автоматическое удаление (см. инструкцию ниже).

При запуске программы, информация о которой была удалена, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready исследует программу как при первом запуске.

Чтобы настроить автоматическое удаление информации о неиспользуемых программах, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.

3. Выполните одно из следующих действий:

- Если вы хотите настроить автоматическое удаление, установите флажок Удалять права для программ, не запускавшихся более N дней и укажите нужное количество дней.

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет удалять информацию о тех программах, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, через заданное количество дней. Также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет удалять информацию о программах, для которых группа доверия и права программы определены автоматически, через 30 дней.

- Если вы хотите выключить автоматическое удаление, снимите флажок Удалять права для программ, не запускавшихся более N дней.

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет хранить информацию о тех программах, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, без ограничений по времени. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет удалять информацию только о программах, для которых группа доверия и права программы определены автоматически, через 30 дней.

4. Сохраните внесенные изменения.

Защита ресурсов операционной системы и персональных данных

Компонент Предотвращение вторжений управляет правами программ на операции над различными категориями ресурсов операционной системы и персональных данных.

Специалисты "Лаборатории Касперского" выделили предустановленные категории защищаемых ресурсов. Вы не можете изменять или удалять предустановленные категории защищаемых ресурсов и относящиеся к ним защищаемые ресурсы.

Вы можете выполнить следующие действия:

- добавить новую категорию защищаемых
- ресурсов; добавить новый защищаемый ресурс;
- выключить защиту ресурса.

Добавление категории защищаемых ресурсов

Чтобы добавить новую категорию защищаемых ресурсов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.
3. Нажмите на кнопку Ресурсы.

   Откроется закладка Защищаемые ресурсы окна Предотвращение вторжений.
4. В левой части закладки Защищаемые ресурсы выберите раздел или категорию защищаемых ресурсов, в которые вы хотите добавить новую категорию защищаемых ресурсов.

5. Нажмите на кнопку Добавить и в раскрывающемся списке выберите элемент Категорию.

   Откроется окно Категория защищаемых ресурсов.

6. В окне Категория защищаемых ресурсов введите название новой категории защищаемых ресурсов.

7. Сохраните внесенные изменения.

Добавление защищаемого ресурса

Чтобы добавить защищаемый ресурс, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.

3. Нажмите на кнопку Ресурсы.

   Откроется закладка Защищаемые ресурсы окна Предотвращение вторжений.

4. В левой части закладки Защищаемые ресурсы выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.

5. Нажмите на кнопку Добавить и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить:

   - Файл или папку.
   - Ключ реестра.

   Откроется окно Защищаемый ресурс.

6. В окне Защищаемый ресурс в поле Название введите название защищаемого ресурса.

7. Нажмите на кнопку Обзор.

8. В открывшемся окне задайте необходимые параметры в зависимости от типа добавляемого защищаемого ресурса и нажмите на кнопку OK.

9. Сохраните внесенные изменения.

Выключение защиты ресурса

Чтобы выключить защиту ресурса, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Продвинутая защита → Предотвращение вторжений.

3. В правой части окна нажмите на кнопку Ресурсы.

   Откроется закладка Защищаемые ресурсы окна Предотвращение вторжений.

4. Выполните одно из следующих действий:

- В левой части закладки в списке защищаемых ресурсов выберите ресурс, защиту которого вы хотите выключить, и снимите флажок рядом с его названием.
- Нажмите на кнопку Исключения и выполните следующие действия:

  a. В окне Исключения нажмите на кнопку Добавить и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить в список исключений из защиты компонента Предотвращение вторжений: Файл или папку или Ключ реестра.

  Откроется окно Защищаемый ресурс.

  b. В окне Защищаемый ресурс в поле Название введите название защищаемого ресурса. c.

  Нажмите на кнопку Обзор.

  d. В открывшемся окне задайте необходимые параметры в зависимости от типа защищаемого ресурса, который вы хотите добавить в список исключений из защиты компонентом Предотвращение вторжений.

  e. Нажмите на кнопку OK.

  f. В окне Защищаемый ресурс нажмите на кнопку OK.

  В списке ресурсов, исключенных из защиты компонента Предотвращение вторжений, появится новый элемент.

  g. В окне Исключения нажмите на кнопку OK.

5. Сохраните внесенные изменения.

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполнить откат действий, произведенных вредоносными программами в операционной системе.

Во время отката действий вредоносной программы в операционной системе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обрабатывает следующие типы активности вредоносной программы:

- Файловая активность

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

  - удаляет исполняемые файлы, созданные вредоносной программой (на всех носителях, кроме сетевых дисков); удаляет исполняемые файлы, созданные программами, в которые внедрилась
  - вредоносная программа; восстанавливает измененные или удаленные вредоносной программой
  - файлы.

  Функциональность восстановления файлов имеет ряд ограничений.

- Реестровая активность

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

  - удаляет разделы и ключи реестра, созданные вредоносной программой; не восстанавливает
  - измененные или удаленные вредоносной программой разделы и ключи реестра.
- Системная активность

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

  - завершает процессы, которые запускала вредоносная программа;
  - завершает процессы, в которые внедрялась вредоносная программа;
  - не возобновляет процессы, которые остановила вредоносная
  - программа.

  Сетевая активность

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие

  - действия: запрещает сетевую активность вредоносной программы; запрещает сетевую
  - активность тех процессов, в которые внедрялась вредоносная программа.

Откат действий вредоносной программы может быть запущен компонентом Защита от файловых угроз, Анализ поведения или при антивирусной проверке.

Откат действий вредоносной программы затрагивает строго ограниченный набор данных. Откат не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

Ограничения функциональности восстановления файлов

Функциональность восстановления файлов имеет следующие ограничения:

- Программа восстанавливает файлы только на устройствах с файловой системой NTFS и FAT32.
- Программа восстанавливает файлы следующих расширений: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Невозможно восстановить файлы, размещенные на сетевых дисках, а также на перезаписываемых CD/DVD-дисках.
- Невозможно восстановить файлы, зашифрованные с помощью Encryption File System (EFS). Подробнее о работе EFS см. на сайте Microsoft.
- Программа не контролирует изменения файлов, выполненные процессами на уровне ядра операционной системы.

- Программа не контролирует изменения файлов, выполненные через сетевой интерфейс (например, файл размещен в папке общего доступа и процесс запущен удаленно с другого компьютера).

Включение и выключение Отката вредоносных действий

Чтобы включить или выключить Откат вредоносных действий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Продвинутая защита → Откат вредоносных действий.
3. Установите флажок Откат вредоносных действий в правой части окна, если вы хотите, чтобы программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready откатывала действия, которые вредоносные программы совершили в операционной системе.
4. Сохраните внесенные изменения.

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз постоянно находится в оперативной памяти компьютера. Компонент проверяет файлы на всех дисках компьютера, а также на подключенных дисках. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент проверяет файлы, к которым обращается пользователь или программа. При обнаружении вредоносного файла Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует операцию с файлом. Далее программа лечит или удаляет вредоносный файл, в зависимости от настройки компонента Защита от файловых угроз.

При обращении к файлу, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready загружает и проверяет содержимое этого файла.

Включение и выключение Защиты от файловых угроз

По умолчанию компонент Защита от файловых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Защиту от файловых угроз при необходимости.

Чтобы включить или выключить Защиту от файловых угроз, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.

3. Выполните одно из следующих действий:

   - Установите флажок Защита от файловых угроз, если вы хотите включить Защиту от файловых угроз.
   - Снимите флажок Защита от файловых угроз, если вы хотите выключить Защиту от файловых угроз.

4. Сохраните внесенные изменения.

Автоматическая приостановка Защиты от файловых угроз

Вы можете настроить автоматическую приостановку Защиты от файловых угроз в указанное время или во время работы с определенными программами.

Приостановка работы Защиты от файловых угроз при конфликте с определенными программами является экстренной мерой. Если во время работы компонента возникают какие-либо конфликты, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (https://companyaccount.kaspersky.com). Специалисты помогут вам наладить совместную работу компонента Защита от файловых угроз с другими программами на вашем компьютере.

Чтобы настроить автоматическую приостановку работы Защиты от файловых угроз, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.
3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно Защита от файловых угроз.
4. В окне Защита от файловых угроз выберите закладку Дополнительно.
5. В блоке Приостановка задачи выполните следующие действия:

   - Установите флажок По расписанию и нажмите на кнопку Расписание, если вы хотите настроить автоматическую приостановку работы Защиты от файловых угроз в указанное время.

     Откроется окно Приостановка задачи.
   - Установите флажок При запуске программ и нажмите на кнопку Выбрать, если вы хотите настроить автоматическую приостановку Защиты от файловых угроз при запуске указанных программ.

     Откроется окно Программы.
6. Выполните одно из следующих действий:

   - Если вы настраиваете автоматическую приостановку Защиты от файловых угроз в указанное время, то в окне Приостановка задачи в полях Приостановить в и Возобновить в укажите время (в формате ЧЧ:ММ), в течение которого Защиту от файловых угроз следует приостанавливать. Нажмите на кнопку ОК.

- Если вы настраиваете автоматическую приостановку Защиты от файловых угроз при запуске указанных программ, то в окне Программы с помощью кнопок Добавить, Изменить и Удалить сформируйте список программ, во время работы которых Защиту от файловых угроз следует приостанавливать. Нажмите на кнопку ОК.

7. Сохраните внесенные изменения.

Изменение уровня безопасности

Для защиты файловой системы компьютера компонент Защита от файловых угроз применяет разные наборы параметров. Такие наборы параметров называют уровнями безопасности. Предустановлены три уровня безопасности: Высокий, Рекомендуемый, Низкий. Параметры уровня безопасности Рекомендуемый считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского". Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

Чтобы изменить уровень безопасности, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.

3. В блоке Уровень безопасности выполните одно из следующих действий:

   - Если вы хотите установить один из предустановленных уровней безопасности (Высокий, Рекомендуемый, Низкий), выберите его при помощи ползунка.

   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку Настройка и задайте параметры в открывшемся окне Защита от файловых угроз.

     После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке Уровень безопасности изменится на Другой.

   - Если вы хотите изменить уровень безопасности на Рекомендуемый, нажмите на кнопку По умолчанию.

4. Сохраните внесенные изменения.

Изменение действия компонента Защита от файловых угроз над зараженными файлами

По умолчанию компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз удаляет эти файлы.

Чтобы изменить действие компонента Защита от файловых угроз над зараженными файлами, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.
3. В блоке Действие при обнаружении угрозы выберите нужный вариант:
   - Лечить; удалять, если лечение невозможно.

     Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз удаляет эти файлы.
   - Лечить; блокировать, если лечение невозможно.

     Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз блокирует эти файлы.
   - Блокировать.

     Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически блокирует зараженные файлы без попытки их вылечить.
4. Сохраните внесенные изменения.

Формирование области защиты компонента Защита от файловых угроз

Под областью защиты подразумеваются объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от файловых угроз являются местоположение и тип проверяемых файлов. По умолчанию компонент Защита от файловых угроз проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков компьютера.

Чтобы сформировать область защиты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.
3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно Защита от файловых угроз.
4. В окне Защита от файловых угроз выберите закладку Общие.
5. В блоке Типы файлов укажите тип файлов, которые вы хотите проверять компонентом Защита от файловых угроз:
   - Выберите Все файлы, если вы хотите проверять все файлы.
   - Выберите Файлы, проверяемые по формату, если вы хотите проверять файлы тех форматов, которые наиболее подвержены заражению.
   - Выберите Файлы, проверяемые по расширению, если вы хотите проверять файлы с расширениями, наиболее подверженными заражению.

Выбирая тип проверяемых файлов, нужно помнить следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, TXT) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, форматы EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.

- Злоумышленник может отправить вирус или другую программу, представляющую угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл пропускается. Если же выбрана проверка файлов по формату, то вне зависимости от расширения компонент Защита от файловых угроз проанализирует заголовок файла, в результате чего может выясниться, что файл имеет формат EXE. Такой файл тщательно проверяется на вирусы и другие программы, представляющие угрозу.

6. В списке Область защиты выполните одно из следующих действий:

   - Нажмите на кнопку Добавить, если вы хотите добавить новый объект в область проверки.

   - Если вы хотите изменить местоположение объекта, выберите объект из области проверки и нажмите на кнопку Изменить.

   Откроется окно Выбор области проверки.

   - Если вы хотите удалить объект из списка проверяемых объектов, выберите объект в списке проверяемых объектов и нажмите на кнопку Удалить.

     Откроется окно подтверждения удаления.

7. Выполните одно из следующих действий:

   - Если вы хотите добавить новый объект или изменить местоположение объекта из списка проверяемых объектов, в окне Выбор области проверки выберите объект и нажмите на кнопку Добавить.

     Все объекты, выбранные в окне Выбор области проверки, отобразятся в списке Область защиты в окне Защита от файловых угроз.

     Нажмите на кнопку OK.

   - Если вы хотите удалить объект, нажмите на кнопку Да в окне подтверждения удаления.

8. Чтобы исключить объект из списка проверяемых объектов, в списке Область защиты снимите флажок рядом с ним. Объект при этом остается в списке проверяемых объектов, но исключается из проверки компонентом Защита от файловых угроз.

9. Сохраните внесенные изменения.

Использование эвристического анализа в работе компонента Защита от файловых угроз

Во время своей работы компонент Защита от файловых угроз использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа компонент Защита от файловых угроз

сравнивает найденный объект с записями в антивирусных базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа компонент Защита от файловых угроз анализирует активность, которую объекты производят в системе. Эвристический анализ позволяет обнаруживать вредоносные объекты, записей о которых еще нет в антивирусных базах программы.

Чтобы настроить использование эвристического анализа в работе компонента Защита от файловых угроз, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.
3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно Защита от файловых угроз.
4. В окне Защита от файловых угроз выберите закладку Производительность.
5. В блоке Методы проверки выполните следующие действия:

   - Если вы хотите, чтобы компонент Защита от файловых угроз использовал эвристический анализ, установите флажок Эвристический анализ и при помощи ползунка задайте уровень эвристического анализа: поверхностный, средний или глубокий.
   - Если вы хотите, чтобы компонент Защита от файловых угроз не использовал эвристический анализ, снимите флажок Эвристический анализ.
6. Сохраните внесенные изменения.

Использование технологий проверки в работе компонента Защита от файловых угроз

Чтобы настроить использование технологий проверки в работе компонента Защита от файловых угроз, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.
3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно Защита от файловых угроз.
4. В окне Защита от файловых угроз выберите закладку Дополнительно.
5. В блоке Технологии проверки выполните следующие действия:

- Установите флажки около названий тех технологий, которые вы хотите использовать в работе компонента Защита от файловых угроз.
- Снимите флажки около названий тех технологий, которые вы не хотите использовать в работе компонента Защита от файловых угроз.

6. Сохраните внесенные изменения.

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов компонентом Защита от файловых угроз: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Вы также можете включить использование технологий iChecker и iSwift, которые позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

Чтобы оптимизировать проверку файлов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.
3. Нажмите на кнопку Настройка.
   Откроется окно Защита от файловых угроз.
4. В окне Защита от файловых угроз выберите закладку Производительность.
5. В блоке Оптимизация проверки установите флажок Проверять только новые и измененные файлы.
6. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы или почтовые базы. Чтобы обнаружить скрытые таким образом вирусы и другие программы, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив скорость проверки.

Способ обработки зараженного составного файла (лечение или удаление) зависит от типа файла.

Компонент Защита от файловых угроз лечит составные файлы форматов RAR, ARJ, ZIP, CAB, LHA и удаляет файлы всех остальных форматов (кроме почтовых баз).

Чтобы настроить проверку составных файлов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.
3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно Защита от файловых угроз.
4. В окне Защита от файловых угроз выберите закладку Производительность.
5. В блоке Проверка составных файлов укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты или файлы офисных форматов.
6. Чтобы проверять только новые и измененные составные файлы, установите флажок Проверять только новые и измененные файлы.

   Компонент Защита от файловых угроз будет проверять только новые и измененные составные файлы всех типов.
7. Нажмите на кнопку Дополнительно.

   Откроется окно Составные файлы.
8. В блоке Фоновая проверка выполните одно из следующих действий:

   - Чтобы запретить компоненту Защита от файловых угроз распаковывать составные файлы в фоновом режиме, снимите флажок Распаковывать составные файлы в фоновом режиме.
   - Чтобы разрешить компоненту Защита от файловых угроз распаковывать составные файлы при проверке в фоновом режиме, установите флажок Распаковывать составные файлы в фоновом режиме и в поле Минимальный размер файла укажите нужное значение.
9. В блоке Ограничение по размеру выполните одно из следующих действий:

   - Чтобы запретить компоненту Защита от файловых угроз распаковывать составные файлы большого размера, установите флажок Не распаковывать составные файлы большого размера и в поле Максимальный размер файла укажите нужное значение. Компонент Защита от файловых угроз не будет распаковывать составные файлы больше указанного размера.
   - Чтобы разрешить компоненту Защита от файловых угроз распаковывать составные файлы большого размера, снимите флажок Не распаковывать составные файлы большого размера.

     Файлом большого размера считается файл, размер которого больше значения в поле Максимальный размер файла.

   Компонент Защита от файловых угроз проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок Не распаковывать составные файлы большого размера.
10. Сохраните внесенные изменения.

Изменение режима проверки файлов

Под режимом проверки подразумевается условие, при котором компонент Защита от файловых угроз начинает проверять файлы. По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует интеллектуальный режим проверки файлов. Работая в этом режиме проверки файлов, компонент Защита от файловых угроз принимает решение о проверке файлов на основании анализа операций, которые пользователь, программа от имени пользователя (под учетными данными которого был осуществлен вход в операционную систему или другого пользователя) или операционная система выполняет над файлами. Например, работая с документом Microsoft O ice Word, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

Чтобы изменить режим проверки файлов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от файловых угроз.
3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно Защита от файловых угроз.
4. В окне Защита от файловых угроз выберите закладку Дополнительно.
5. В блоке Режим проверки выберите нужный режим:
   - Интеллектуальный.
   - При доступе и изменении.
   - При доступе.
   - При выполнении.
6. Сохраните внесенные изменения.

Защита от веб-угроз

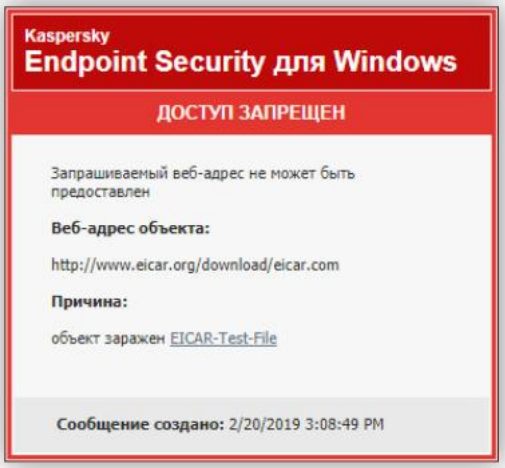
Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует вредоносные и фишинговые веб-сайты. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет HTTP-, HTTPS- и FTP-трафик. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет URL- и IP-адреса. Вы можете задать порты, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет контролировать, или выбрать все порты.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

При попытке пользователя открыть вредоносный или фишинговый веб-сайт, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует доступ и покажет предупреждение (см. рис. ниже).



Сообщение о запрете доступа к веб-сайту

Включение и выключение Защиты от веб-угроз

По умолчанию компонент Защита от веб-угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить компонент Защита от веб-угроз при необходимости.

Чтобы включить или выключить компонент Защита от веб-угроз выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от веб-угроз.
3. Выполните одно из следующих действий:
   - Установите флажок Защита от веб-угроз, если вы хотите включить компонент Защита от веб-угроз.
   - Снимите флажок Защита от веб-угроз, если вы хотите выключить компонент Защита от веб-угроз.
4. Сохраните внесенные изменения.

Изменение уровня безопасности веб-трафика

Для защиты данных, получаемых и передаваемых по протоколам HTTP и FTP, компонент Защита от веб-угроз применяет разные наборы параметров. Такие наборы параметров называются уровнями безопасности веб-

трафика. Предустановлены три уровня безопасности веб-трафика: Высокий, Рекомендуемый, Низкий. Параметры уровня безопасности веб-трафика Рекомендуемый считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского". Вы можете выбрать один из предустановленных уровней безопасности веб-трафика, получаемых или передаваемых по протоколам HTTP и FTP, или настроить уровень безопасности веб-трафика самостоятельно. После того как вы изменили параметры уровня безопасности веб-трафика, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности веб-трафика.

Чтобы изменить уровень безопасности веб-трафика, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от веб-угроз.
3. В блоке Уровень безопасности выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности веб-трафика (Высокий, Рекомендуемый, Низкий), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности веб-трафика самостоятельно, нажмите на кнопку Настройка и задайте параметры в открывшемся окне Защита от веб-угроз.

     После того как вы самостоятельно настроили уровень безопасности веб-трафика, название уровня безопасности веб-трафика в блоке Уровень безопасности изменится на Другой.
   - Если вы хотите изменить настроенный самостоятельно уровень безопасности веб-трафика на Рекомендуемый, нажмите на кнопку По умолчанию.
4. Сохраните внесенные изменения.

Изменение действия над вредоносными объектами веб-трафика

По умолчанию в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и выводит на экран окно уведомления о блокировке.

Чтобы изменить действие над вредоносными объектами веб-трафика, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от веб-угроз.
3. В блоке Действие при обнаружении угрозы выберите вариант действия, которое Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет над вредоносными объектами веб-трафика:
   - Запрещать загрузку.

     Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и выводит на экран окно уведомления о блокировке, создает в журнале запись, содержащую информацию о зараженном объекте.
   - Информировать.

Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз разрешает загрузку этого объекта на компьютер и Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает в журнале запись, содержащую информацию о зараженном объекте, добавляет информацию о зараженном объекте в список активных угроз.

4. Сохраните внесенные изменения.

Проверка компонентом Защита от веб-угроз ссылок по базам фишинговых и вредоносных веб-адресов

Проверка ссылок на принадлежность к фишинговым веб-адресам позволяет избежать фишинговых атак. Частным примером фишинговых атак может служить сообщение электронной почты якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт банка в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его вебадрес в браузере, однако находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

Поскольку ссылка на фишинговый веб-сайт может содержаться не только в сообщении электронной почты, но и, например, в тексте ICQ-сообщения, компонент Защита от веб-угроз отслеживает попытки перейти на фишинговый веб-сайт на уровне проверки веб-трафика и блокирует доступ к таким веб-сайтам. Списки фишинговых веб-адресов включены в комплект поставки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Чтобы настроить проверку компонентом Защита от веб-угроз ссылок по базам фишинговых и вредоносных веб-адресов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от веб-угроз.
3. Нажмите на кнопку Настройка.

   Откроется окно Защита от веб-угроз.
4. В окне Защита от веб-угроз выберите закладку Общие.
5. Выполните следующие действия:

   - В блоке Методы проверки установите флажок Проверять ссылки по базе вредоносных веб-адресов, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам вредоносных вебадресов.

     Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет ссылки по базам вредоносных веб-адресов, даже если сетевой трафик передается по защищенному соединению и флажок Проверять защищенные соединения снят.

   - В блоке Параметры антифишинга установите флажок Проверять ссылки по базе фишинговых вебадресов, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам фишинговых веб-адресов.

Для проверки ссылок вы также можете использовать репутационные базы Kaspersky Security Network.

6. Сохраните внесенные изменения.

Использование эвристического анализа в работе компонента Защита от веб-угроз

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready анализирует активность, которую программы производят в операционной системе. Эвристический анализ позволяет обнаруживать угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Чтобы настроить использование эвристического анализа, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от веб-угроз.
3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно Защита от веб-угроз.
4. Выберите закладку Общие.
5. Если вы хотите, чтобы компонент Защита от веб-угроз использовал эвристический анализ при проверке веб-трафика на наличие вирусов и других программ, представляющих угрозу, в блоке Методы проверки установите флажок Эвристический анализ для обнаружения вирусов и при помощи ползунка задайте уровень эвристического анализа: поверхностный, средний или глубокий.
6. Если вы хотите, чтобы компонент Защита от веб-угроз использовал эвристический анализ при проверке веб-страниц на наличие фишинговых ссылок, в блоке Параметры антифишинга установите флажок Эвристический анализ для обнаружения фишинговых ссылок.
7. Сохраните внесенные изменения.

Формирование списка доверенных веб-адресов

Вы можете сформировать список веб-адресов, содержанию которых вы доверяете. Компонент Защита от веб-угроз не анализирует информацию, поступающую с доверенных веб-адресов, на присутствие вирусов и других программ, представляющих угрозу. Такая возможность может быть использована, например, в том случае, если компонент Защита от веб-угроз препятствует загрузке файла с известного вам веб-сайта.

Под веб-адресом подразумевается адрес как отдельной веб-страницы, так и веб-сайта.

Чтобы сформировать список доверенных веб-адресов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от веб-угроз.
3. Нажмите на кнопку Настройка.

   Откроется окно Защита от веб-угроз.
4. Выберите закладку Доверенные веб-адреса.
5. Установите флажок Не проверять веб-трафик с доверенных веб-адресов.
6. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете. Для пополнения списка выполните следующие действия:

   a. Нажмите на кнопку Добавить.

      Откроется окно Веб-адрес / Маска веб-адреса.

   b. Введите адрес веб-сайта / веб-страницы или маску адреса веб-сайта / веб-страницы. с.

      Нажмите на кнопку OK.

      В списке доверенных веб-адресов появится новая запись.
7. Сохраните внесенные изменения.

Защита от почтовых угроз

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других программ, представляющих угрозу. Также компонент проверяет сообщения на наличие вредоносных и фишинговых ссылок. По умолчанию компонент Защита от почтовых угроз постоянно находится в оперативной памяти компьютера и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, NNTP или в почтовом клиенте Microsoft O ice Outlook (MAPI). Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready переименовывает тему сообщения: `[Сообщение заражено] <тема сообщения>` или `[Зараженный объект удален] <тема сообщения>`.

Компонент взаимодействует с почтовыми клиентами, установленными на компьютере. Для почтового клиента Microsoft O ice Outlook предусмотрено расширение с дополнительными параметрами. Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft O ice Outlook во время установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Включение и выключение Защиты от почтовых угроз

По умолчанию компонент Защита от почтовых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме.

Чтобы включить или выключить компонент Защита от почтовых угроз выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от почтовых угроз.
3. Выполните одно из следующих действий:
   - Установите флажок Защита от почтовых угроз, если вы хотите включить компонент Защита от почтовых угроз.
   - Снимите флажок Защита от почтовых угроз, если вы хотите выключить компонент Защита от почтовых угроз.
4. Сохраните внесенные изменения.

Изменение уровня безопасности почты

Для защиты почты компонент Защита от почтовых угроз применяет разные наборы параметров. Такие наборы параметров называют уровнями безопасности почты. Установлены три уровня безопасности почты: Высокий, Рекомендуемый, Низкий. Параметры уровня безопасности почты Рекомендуемый считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского". Вы можете выбрать один из предустановленных уровней безопасности почты или настроить уровень безопасности почты самостоятельно. После того как вы изменили параметры уровня безопасности почты, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности почты.

Чтобы изменить уровень безопасности почты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от почтовых угроз.
3. В блоке Уровень безопасности выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности почты (Высокий, Рекомендуемый, Низкий), выберите его при помощи ползунка.

- Если вы хотите настроить уровень безопасности почты самостоятельно, нажмите на кнопку Настройка и задайте параметры в открывшемся окне Защита от почтовых угроз.

  После того как вы самостоятельно настроили уровень безопасности почты, название уровня безопасности почты в блоке Уровень безопасности изменится на Другой.

- Если вы хотите изменить настроенный самостоятельно уровень безопасности почты на Рекомендуемый, нажмите на кнопку По умолчанию.

4. Сохраните внесенные изменения.

Изменение действия над зараженными сообщениями электронной почты

По умолчанию компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз удаляет зараженные сообщения электронной почты.

Чтобы изменить действие над зараженными сообщениями электронной почты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Защита от почтовых угроз.

3. В блоке Действие при обнаружении угрозы выберите вариант действия, которое выполняет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready при обнаружении зараженного сообщения:

   - Лечить; удалять, если лечение невозможно.

     Если выбран этот вариант действия, то компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз удаляет зараженные сообщения электронной почты.

   - Лечить; блокировать, если лечение невозможно.

     Если выбран этот вариант действия, то компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз блокирует зараженные сообщения электронной почты.

   - Блокировать.

     Если выбран этот вариант действия, то компонент Защита от почтовых угроз автоматически блокирует зараженные сообщения электронной почты без попытки их вылечить.

4. Сохраните внесенные изменения.

Формирование области защиты компонента Защита от почтовых угроз

Область защиты – это объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от почтовых угроз являются параметры интеграции компонента Защита от почтовых угроз в почтовые клиенты, тип сообщений электронной почты и почтовые протоколы, трафик которых проверяет компонент Защита от почтовых угроз. По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет как входящие, так и исходящие сообщения электронной почты, трафик почтовых протоколов POP3, SMTP, NNTP и IMAP, а также интегрируется в почтовый клиент Microsoft Oice Outlook.

Чтобы сформировать область защиты компонента Защита от почтовых угроз, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от почтовых угроз.
3. Нажмите на кнопку Настройка.

   Откроется окно Защита от почтовых угроз.
4. Выберите закладку Общие.
5. В блоке Область защиты выполните одно из следующих действий:

   - Выберите вариант Входящие и исходящие сообщения, если вы хотите, чтобы компонент Защита от почтовых угроз проверял все входящие и исходящие сообщения на вашем компьютере.
   - Выберите вариант Только входящие сообщения, если вы хотите, чтобы компонент Защита от почтовых угроз проверял только входящие сообщения на вашем компьютере.

     Если вы выбираете проверку только входящих сообщений, рекомендуется однократно проверить все исходящие сообщения, поскольку существует вероятность того, что на вашем компьютере есть почтовые черви, которые используют электронную почту в качестве канала распространения. Это позволит избежать проблем, связанных с неконтролируемой рассылкой зараженных сообщений с вашего компьютера.
6. В блоке Встраивание в систему выполните следующие действия:

   - Установите флажок Трафик POP3 / SMTP / NNTP / IMAP, если вы хотите, чтобы компонент Защита от почтовых угроз проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя.

     Снимите флажок Трафик POP3 / SMTP / NNTP / IMAP, если вы хотите, чтобы компонент Защита от почтовых угроз не проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя. В этом случае сообщения проверяет расширение компонента Защита от почтовых угроз, встроенное в почтовый клиент Microsoft O ice Outlook, после их получения на компьютере пользователя, если установлен флажок Дополнительно: расширение в Microsoft O ice Outlook.

Если вы используете почтовый клиент, отличный от Microsoft Oice Outlook, то при снятом флажке Трафик POP3 / SMTP / NNTP / IMAP компонент Защита от почтовых угроз не проверяет сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.

- Установите флажок Дополнительно: расширение в Microsoft O ice Outlook, если вы хотите открыть доступ к настройке параметров компонента Защита от почтовых угроз из программы Microsoft O ice Outlook и включить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и

  MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в программу Microsoft O ice Outlook.

  Снимите флажок Дополнительно: расширение в Microsoft O ice Outlook, если вы хотите закрыть доступ к настройке параметров компонента Защита от почтовых угроз из программы Microsoft O ice Outlook и выключить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в программу Microsoft O ice Outlook.

Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft O ice Outlook во время установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

7. Сохраните внесенные изменения.

Проверка составных файлов, вложенных в сообщения электронной почты

Вы можете включить или выключить проверку объектов, вложенных в сообщения, ограничить максимальный размер проверяемых объектов, вложенных в сообщения, и максимальную длительность проверки объектов, вложенных в сообщения.

Чтобы настроить проверку составных файлов, вложенных в сообщения электронной почты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от почтовых угроз.
3. Нажмите на кнопку Настройка.

   Откроется окно Защита от почтовых угроз.
4. Выберите закладку Общие.
5. В блоке Проверка составных файлов выполните следующие действия:

   - Снимите флажок Проверять вложенные архивы, если вы хотите, чтобы компонент Защита от почтовых угроз не выполнял проверку вложенных в сообщения архивов.

- Снимите флажок Проверять вложенные файлы офисных форматов, если вы хотите, чтобы компонент Защита от почтовых угроз не выполнял проверку вложенных в сообщения файлов офисных форматов.

- Установите флажок Не проверять архивы размером более N МБ, если вы хотите, чтобы компонент Защита от почтовых угроз не проверял вложенные в сообщения архивы размером более N мегабайт. Если вы установили этот флажок, укажите максимальный размер архивов в поле рядом с названием флажка.

- Снимите флажок Не проверять архивы более N с, если вы хотите, чтобы компонент Защита от почтовых угроз проверял вложенные в сообщения архивы, если на их проверку затрачивается более N секунд.

6. Сохраните внесенные изменения.

Фильтрация вложений в сообщениях электронной почты

Функциональность фильтрации вложений не применяется для исходящих сообщений электронной почты.

Вредоносные программы могут распространяться в виде вложений в сообщениях электронной почты. Вы можете настроить фильтрацию по типу вложений в сообщениях, чтобы автоматически переименовывать или удалять файлы указанных типов. Переименовав вложение определенного типа, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready может защитить ваш компьютер от автоматического запуска вредоносной программы.

Чтобы настроить фильтрацию вложений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Защита от почтовых угроз.

3. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно Защита от почтовых угроз.

4. В окне Защита от почтовых угроз выберите закладку Фильтр вложений.

5. Выполните одно из следующих действий:

   - Выберите вариант Не применять фильтр, если вы хотите, чтобы компонент Защита от почтовых угроз не фильтровал вложения в сообщениях.

   - Выберите вариант Переименовывать вложения указанных типов, если вы хотите, чтобы компонент Защита от почтовых угроз изменял названия вложенных в сообщения файлов указанных типов.

   - Выберите вариант Удалять вложения указанных типов, если вы хотите, чтобы компонент Защита от почтовых угроз удалял вложенные в сообщения файлы указанных типов.

6. Если на предыдущем шаге инструкции вы выбрали вариант Переименовывать вложения указанных типов или вариант Удалять вложения указанных типов, установите флажки напротив нужных типов файлов.

7. Сохраните внесенные изменения.

Проверка почты в Microsoft Oice Outlook

Во время установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в программу Microsoft O ice Outlook (далее также "Outlook") встраивается расширение компонента Защита от почтовых угроз. Оно позволяет перейти к настройке параметров компонента Защита от почтовых угроз из программы Outlook, а также указать, в какой момент проверять сообщения электронной почты на присутствие вирусов и других программ, представляющих угрозу. Расширение компонента Защита от почтовых угроз для Outlook может проверять входящие и исходящие сообщения, переданные по протоколам POP3, SMTP, NNTP, IMAP и MAPI. Также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает работу с другими почтовыми клиентами (в том числе с Microsoft Outlook Express®, Windows Mail и Mozilla™ Thunderbird™).

Работая с почтовым клиентом Mozilla Thunderbird, компонент Защита от почтовых угроз не проверяет на вирусы и другие программы, представляющие угрозу, сообщения, передаваемые по протоколу IMAP, в случае если используются фильтры, перемещающие сообщения из папки Входящие.

В программе Outlook входящие сообщения сначала проверяет компонент Защита от почтовых угроз (если в интерфейсе программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлен флажок Трафик
POP3 / SMTP / NNTP / IMAP), затем входящие сообщения проверяет расширение компонента Защита от почтовых угроз для Outlook. Если компонент Защита от почтовых угроз обнаруживает в сообщении вредоносный объект, он уведомляет вас об этом.

Настройка параметров компонента Защита от почтовых угроз из программы Outlook доступна в том случае, если в интерфейсе программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлен флажок Дополнительно: расширение в Microsoft O ice Outlook.

Исходящие сообщения сначала проверяет расширение компонента Защита от почтовых угроз для Outlook, а затем проверяет компонент Защита от почтовых угроз.

Настройка проверки почты в программе Outlook

Чтобы перейти к настройке проверки почты в программе Outlook 2007, выполните следующие действия:

1. Откройте главное окно Outlook 2007.
2. В меню программы выберите пункт Сервис → Параметры.

   Откроется окно Параметры.
3. В окне Параметры выберите закладку Защита почты.

Чтобы перейти к настройке проверки почты в программе Outlook 2010 / 2013 / 2016, выполните следующие действия:

1. Откройте главное окно Outlook.

В верхнем левом углу выберите закладку Файл.

2. Нажмите на кнопку Параметры.

   Откроется окно Параметры Outlook.

3. Выберите раздел Надстройки.

   В правой части окна отобразятся параметры встроенных в Outlook плагинов.

4. Нажмите на кнопку Параметры надстроек.

Настройка проверки почты с помощью Kaspersky Security Center

В случае проверки почты с помощью расширения компонента Защита от почтовых угроз для Outlook рекомендуется использовать режим кеширования сервера Exchange (Use Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендациях по его использованию вы можете найти в базе знаний Майкрософт: https://technet.microsoft.com/ru-ru/library/cc179175.aspx

Чтобы настроить режим работы расширения компонента Защита от почтовых угроз для Outlook с помощью Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку Политики.

4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

5. В окне политики выберите Базовая защита → Защита от почтовых угроз.

6. В блоке Уровень безопасности нажмите на кнопку Настройка.

   Откроется окно Защита от почтовых угроз.

7. В блоке Встраивание в систему нажмите на кнопку Настройка.

8. В окне Защита почты выполните следующие действия:

   - Установите флажок Проверять при получении, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло входящие сообщения в момент их поступления в почтовый ящик.

   - Установите флажок Проверять при прочтении, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло входящие сообщения в тот момент, когда пользователь открывает их для чтения.

   - Установите флажок Проверять при отправке, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло исходящие сообщения в момент их отправки.

9. Сохраните внесенные изменения.

Защита от сетевых угроз

Компонент Защита от сетевых угроз (англ. IDS – Intrusion Detection System) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует сетевое соединение с атакующим компьютером.

Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей программы.

Включение и выключение Защиты от сетевых угроз

По умолчанию Защита от сетевых угроз включена и работает в оптимальном режиме. При необходимости вы можете выключить Защиту от сетевых угроз.

Чтобы включить или выключить Защиту от сетевых угроз выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от сетевых угроз.
3. Выполните следующие действия:
   - Установите флажок Защита от сетевых угроз, если вы хотите включить Защиту от сетевых угроз.
   - Снимите флажок Защита от сетевых угроз, если вы хотите выключить Защиту от сетевых угроз.
4. Сохраните внесенные изменения.

Изменение параметров блокирования атакующего компьютера

Чтобы изменить параметры блокирования атакующего компьютера, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от сетевых угроз.
3. Установите флажок Добавить атакующий компьютер в список блокирования на.

   Если этот флажок установлен, то, обнаружив попытку сетевой атаки, компонент Защита от сетевых угроз блокирует сетевую активность атакующего компьютера в течение заданного времени, чтобы автоматически защитить компьютер от возможных будущих сетевых атак с этого адреса.

   Если этот флажок снят, то, обнаружив попытку сетевой атаки, компонент Защита от сетевых угроз не включает автоматическую защиту от возможных будущих сетевых атак с этого адреса.

4. Измените время блокирования атакующего компьютера в поле, расположенном справа от флажка Добавить атакующий компьютер в список блокирования на.

5. Сохраните внесенные изменения.

Настройка адресов исключений из блокирования

Чтобы настроить адреса исключений из блокирования, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Защита от сетевых угроз.

3. Нажмите на кнопку Исключения.

   Откроется окно Исключения.

4. Выполните одно из следующих действий:

   - Если хотите добавить новый IP-адрес, нажмите на кнопку Добавить.

   - Если хотите изменить добавленный ранее IP-адрес, выберите его в списке адресов и нажмите на кнопку Изменить.

   Откроется окно IP-адрес.

5. Введите IP-адрес компьютера, сетевые атаки с которого не должны блокироваться.

6. Сохраните внесенные изменения.

Защита от атак типа MAC-спуфинг

Компонент Защита от сетевых угроз отслеживает уязвимости в протоколе определения адреса (англ. Address Resolution Protocol – ARP). Таким образом компонент защищает компьютер от атак типа MACспуфинг. Атака типа MAC-спуфинг заключается в изменении MAC-адреса сетевого устройства (сетевой карты). В результате злоумышленник может перенаправить данные, отправленные на устройство, на другое устройство и получить доступ к этим данным.

По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не отслеживает атаки типа MAC-спуфинг.

Чтобы изменить режим работы защиты от атак типа MAC-спуфинг, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Защита от сетевых угроз.

3. В блоке Режим работы защиты от атак типа MAC-спуфинг выберите один из следующих вариантов:

- Не отслеживать атаки типа MAC-спуфинг.
- Уведомлять обо всех признаках атак типа MAC-спуфинг.
- Блокировать все признаки атак типа MAC-спуфинг.

Проверка защищенных соединений

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

После установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов.Также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready включает использование системного хранилища доверенных сертификатов в программах Firefox и Thunderbird для проверки трафика этих программ.

Компоненты Веб-Контроль, Защита от почтовых угроз, Защита от веб-угроз могут расшифровывать и проверять сетевой трафик, передаваемый по защищенным соединениям с использованием следующих протоколов: SSL 3.0;

- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.
-

Настройка параметров проверки защищенных соединений

Чтобы настроить параметры проверки защищенных соединений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры сети.
3. Установите флажок Проверять защищенные соединения, если вы хотите, чтобы программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролировала зашифрованный сетевой трафик.
4. Если требуется, добавьте исключения из проверки: доверенные адреса и программы.
5. Нажмите на кнопку Дополнительные параметры.
6. Настройте параметры проверки проверки защищенных соединений (см. таблицу ниже).
7. Сохраните внесенные изменения.

Параметры проверки защищенных соединений

Параметр	Описание
При переходе на домен с недоверенным сертификатом разрешает	• Разрешать. Если выбран этот вариант, то при переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установку сетевого соединения. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения. По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу. После перехода по этой ссылке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в течение часа не будет отображать предупреждения о недоверенном сертификате при переходе на другие веб-ресурсы в том же домене. • Блокировать соединение. Если выбран этот вариант, то при переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует сетевое соединение. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображает HTML-страницу с информацией о причине, по которой переход на этот домен заблокирован.
При возникновении ошибок проверки защищенных соединений	• Блокировать соединение. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует это сетевое соединение. • Добавлять домен в исключения. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавляет домен, при переходе на который возникла ошибка, в список доменов с ошибками проверки и не контролирует зашифрованный сетевой трафик при переходе на этот домен. Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе программы. Чтобы сбросить содержание списка, нужно выбрать элемент Блокировать соединение.
Блокировать соединение по протоколу SSL 2.0	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0, и не контролирует сетевой трафик, передаваемый по этим соединениям.

Расшифровать защищенное соединение с сайтом, использующим EVсертификат	EV-сертификаты (англ. Extended Validation Certi cate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет. Если флажок установлен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не имеет доступа к содержанию HTTPS-трафика. Поэтому программа контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://facebook.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.

Исключение защищенных соединений из проверки

Большинство веб-ресурсов используют защищенное соединение. Специалисты "Лаборатории Касперского" рекомендуют включить проверку защищенных соединений. Если проверка защищенных соединений мешает работе, вы можете добавить веб-сайт в исключения, – доверенные адреса. Если доверенная программа использует защищенное соединение, вы можете выключить проверку защищенных соединений для этой программы. Например, вы можете выключить проверку защищенных соединений для программ облачных хранилищ, так как эти программы используют двухфакторную аутентификацию с собственным сертификатом.

Чтобы исключить веб-адрес из проверки защищенных соединений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры сети.
3. В блоке Проверка защищенных соединений нажмите на кнопку Доверенные адреса.
4. Нажмите на кнопку Добавить.
5. Введите имя домена или IP-адрес, если вы хотите, чтобы программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяла защищенные соединения, устанавливаемые при переходе на эту веб-страницу.
6. Сохраните внесенные изменения.

По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет защищенные соединения при возникновении ошибок и добавляет веб-сайт в специальный список – домены с ошибками проверки. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready составляет список для каждого пользователя отдельно и не передает данные в Kaspersky Security Center. Вы можете включить блокирование соединения при возникновении ошибки. Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе программы.

Чтобы просмотреть список доменов с ошибками проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Параметры сети.

3. В блоке Проверка защищенных соединений нажмите на кнопку Дополнительные параметры.

4. В открывшемся окне нажмите на ссылку Домены с ошибками проверки.

Откроется список доменов с ошибками проверки. Чтобы сбросить список вам нужно включить блокирование соединения при возникновении ошибки в политике, применить политику, вернуть параметр в исходное состояние и снова применить политику.

Специалисты "Лаборатории Касперского" составляют список доверенных веб-сайтов, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет независимо от параметров программы, – глобальные исключения.

Чтобы просмотреть глобальные исключения из проверки защищенного трафика, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Параметры сети.

3. В блоке Проверка защищенных соединений нажмите на ссылку сайтах.

Откроется окно Глобальные исключения проверки зашифрованного трафика. В окне отображается составленная специалистами "Лаборатории Касперского" таблица с информацией о сайтах и программах, для которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет защищенные соединения. Таблица может быть обновлена при обновлении баз и модулей Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Сетевой экран

Сетевой экран блокирует несанкционированные подключения к компьютеру во время работы в интернете или локальной сети. Также Сетевой экран контролирует сетевую активность программ на компьютере. Это позволяет защитить локальную сеть организации от кражи персональных данных и других атак. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и предустановленных сетевых правил.

Сетевые правила

Вы можете настроить сетевые правила на следующих уровнях:

- Сетевые пакетные правила. Используются для ввода ограничений на сетевые пакеты независимо от программы. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready имеет предустановленные сетевые пакетные правила с разрешениями, рекомендованными специалистами "Лаборатории Касперского".

- Сетевые правила программ. Используются для ограничения сетевой активности конкретной программы. Учитываются не только характеристики сетевого пакета, но и конкретная программа, которой адресован этот сетевой пакет, либо которая инициировала отправку этого сетевого пакета.

Контроль доступа программ к ресурсам операционной системы, процессам и персональным данным обеспечивает компонент Предотвращение вторжений с помощью прав программ.

Во время первого запуска программы Сетевой экран выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.

2. Проверяет безопасность программы в Kaspersky Security Network.

   Для более эффективной работы Сетевого экрана вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает программу в одну из групп доверия: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

   Группа доверия определяет права, которые Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready использует для контроля сетевой активности программ. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

   Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает программу в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

   Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует сетевую активность программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещены любые сетевые соединения.

При следующем запуске программы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие сетевые правила. Если программа была изменена, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready исследует программу как при первом запуске.

Приоритеты сетевых правил

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если сетевая активность добавлена в несколько правил, Сетевой экран регулирует сетевую активность по правилу с высшим приоритетом.

Сетевые пакетные правила имеют более высокий приоритет, чем сетевые правила программ. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила программ, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Сетевые пакетные правила имеют более высокий приоритет, чем сетевые правила программ. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила программ, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Сетевые правила программ имеют особенность. Сетевые правило программ включает в себя правила доступа по статусу сети: публичная, локальная, доверенная. Например, для группы доверия "Сильные ограничения" по умолчанию запрещена любая сетевая активность программы в сетях всех статусов. Если для отдельной программы (родительская программа) задано сетевое правило, то дочерние процессы других программ будут выполнены в соответствии с сетевым правилом родительской программы. Если сетевое правило для программы отсутствует, дочерние процессы будут выполнены в соответствии с правилом доступа к сетям группы доверия.

Например, вы запретили любую сетевую активность всех программ для сетей всех статусов, кроме браузера X. Если в браузере X (родительская программа) запустить установку браузера Y (дочерний процесс), то установщик браузера Y получит доступ к сети и загрузит необходимые файлы. После установки браузеру Y будут запрещены любые сетевые соединения в соответствии с параметрами Сетевого экрана. Чтобы запретить установщику браузера Y сетевую активность в качестве дочернего процесса, необходимо добавить сетевое правило для установщика браузера Y.

Статусы сетевых соединений

Сетевой экран позволяет контролировать сетевую активность в зависимости от статуса сетевого соединения. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready получает статус сетевого соединения от операционной системы компьютера. Статус сетевого соединения в операционной системе задает пользователь при настройке подключения. Вы можете изменить статус сетевого соединения в параметрах Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Сетевой экран будет контролировать сетевую активность в зависимости от статуса сети в параметрах Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, а не операционной системы.

Выделены следующие статусы сетевого соединения:

- Публичная сеть. Сеть не защищена антивирусными программами, сетевыми экранами, фильтрами (например, Wi-Fi в кафе). Пользователю компьютера, подключенного к такой сети, Сетевой экран закрывает доступ к файлам и принтерам этого компьютера. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу этого компьютера. Сетевой экран фильтрует сетевую активность каждой программы в соответствии с сетевыми правилами этой программы.

  Сетевой экран по умолчанию присваивает статус Публичная сеть сети Интернет. Вы не можете изменить статус сети Интернет.

- Локальная сеть. Сеть для пользователей, которым ограничен доступ к файлам и принтерам этого компьютера (например, для локальной сети организации или для домашней сети).

Доверенная сеть. Безопасная сеть, во время работы в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. Для сетей с этим статусом Сетевой экран разрешает любую сетевую активность в рамках этой сети.

Включение и выключение Сетевого экрана

По умолчанию Сетевой экран включен и работает в оптимальном режиме.

Чтобы включить или выключить Сетевой экран выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.

3. Выполните одно из следующих действий:

   - Установите флажок Сетевой экран, если вы хотите включить Сетевой экран.
   - Снимите флажок Сетевой экран, если вы хотите выключить Сетевой экран.

4. Сохраните внесенные изменения.

Изменение статуса сетевого соединения

Чтобы изменить статус сетевого соединения, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.

3. Нажмите на кнопку Доступные сети.

   Откроется окно Сетевой экран.

4. Выберите сетевое соединение, статус которого вы хотите изменить.

5. В контекстном меню выберите статус сетевого соединения:

   - Публичная сеть.
   - Локальная сеть.
   - Доверенная сеть.

6. Сохраните внесенные изменения.

Работа с сетевыми пакетными правилами

Вы можете выполнить следующие действия в процессе работы с сетевыми пакетными правилами:

- Создать новое сетевое пакетное правило.

  Вы можете создать новое сетевое пакетное правило, сформировав набор условий и действий над сетевыми пакетами и потоками данных.

- Включить и выключить сетевое пакетное правило.

  Все сетевые пакетные правила, созданные Сетевым экраном по умолчанию, имеют статус Включено. Если сетевое пакетное правило включено, Сетевой экран применяет это правило.

  Вы можете выключить любое сетевое пакетное правило, выбранное в списке сетевых пакетных правил. Если сетевое пакетное правило выключено, Сетевой экран временно не применяет это правило.

Новое сетевое пакетное правило, созданное пользователем, по умолчанию добавляется в список сетевых пакетных правил со статусом Включено.

- Изменить параметры существующего сетевого пакетного правила.

  После того как вы создали новое сетевое пакетное правило, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Изменить действие Сетевого экрана для сетевого пакетного правила.

  В списке сетевых пакетных правил вы можете изменить действие, которое Сетевой экран выполняет, обнаружив сетевую активность указанного сетевого пакетного правила.

- Изменить приоритет сетевого пакетного правила.

  Вы можете повысить или понизить приоритет выбранного в списке сетевого пакетного правила.

- Удалить сетевое пакетное правило.

  Вы можете удалить сетевое пакетное правило, если вы не хотите, чтобы Сетевой экран применял это правило при обнаружении сетевой активности, и чтобы оно отображалось в списке сетевых пакетных правил со статусом Выключено.

Создание и изменение сетевого пакетного правила

Создавая сетевые пакетные правила, следует помнить, что они имеют приоритет над сетевыми правилами программ.

Чтобы создать или изменить сетевое пакетное правило, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.
3. Нажмите на кнопку Сетевые пакетные правила.
4. Откроется окно Сетевой экран на закладке Сетевые пакетные правила.

   На этой закладке представлен список сетевых пакетных правил, установленных Сетевым экраном по умолчанию.
5. Выполните одно из следующих действий:

   - Если хотите создать новое сетевое пакетное правило, нажмите на кнопку Добавить.
   - Если хотите изменить сетевое пакетное правило, выберите его в списке сетевых пакетных правил и нажмите на кнопку Изменить.

   Откроется окно Сетевое правило.

.

6 В раскрывающемся списке Действие выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:

- Разрешать.
- Запрещать.
- По правилам программы.

7. В поле Название укажите название сетевой службы одним из следующих способов:

- Нажмите на значок , расположенный справа от поля Название, и в раскрывающемся списке выберите название сетевой службы.

  В раскрывающийся список входят сетевые службы, описывающие наиболее часто используемые сетевые соединения.

- В поле Название введите название сетевой службы вручную.

8. Укажите протокол передачи данных:

a. Установите флажок Протокол.

b. В раскрывающемся списке выберите тип протокола, по которому следует контролировать сетевую активность.

Сетевой экран контролирует соединения по протоколам TCP, UDP, ICMP, ICMPv6, IGMP и GRE. Если сетевая служба выбрана в раскрывающемся списке Название, то флажок Протокол устанавливается автоматически и в раскрывающемся списке рядом с флажком выбирается тип протокола, который соответствует выбранной сетевой службе. По умолчанию флажок Протокол снят.

9. В раскрывающемся списке Направление выберите направление контролируемой сетевой активности.

Сетевой экран контролирует сетевые соединения со следующими направлениями:

- Входящее (пакет).
- Входящее.
- Входящее / Исходящее.
- Исходящее (пакет).
- Исходящее.

10. Если в качестве протокола выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета:

a. Установите флажок ICMP-тип и в раскрывающемся списке выберите тип ICMP-пакета.

b. Установите флажок ICMP-код и в раскрывающемся списке выберите код ICMP-пакета.

11. Если в качестве протокола выбран протокол TCP или UDP, вы можете через запятую указать номера портов компьютера пользователя и удаленного компьютера, соединение между которыми следует контролировать:

a. В поле Удаленные порты введите порты удаленного компьютера.

b. В поле Локальные порты введите порты компьютера пользователя.

12 В таблице Сетевые адаптеры укажите параметры сетевых адаптеров, с которых могут быть отправлены или которыми могут быть приняты сетевые пакеты. Для этого воспользуйтесь кнопками Добавить, Изменить и Удалить.

13. Если вы хотите ограничить контроль сетевых пакетов по времени их жизни (TTL, Time to Live), установите флажок Время жизни (TTL) и в поле рядом укажите диапазон значений времени жизни передаваемых и / или получаемых сетевых пакетов.

Сетевое правило будет контролировать передачу сетевых пакетов, у которых время жизни не превышает указанного значения.

В противном случае снимите флажок Время жизни (TTL).

14. Укажите сетевые адреса удаленных компьютеров, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке Удаленные адреса выберите одно из следующих значений:

- Любой адрес. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.
- Адреса подсети. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, относящимися к выбранному типу сети: Доверенные сети, Локальные сети, Публичные сети.
- Адреса из списка. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, которые можно указать в списке ниже с помощью кнопок Добавить, Изменить и Удалить.

15. Укажите сетевые адреса компьютеров с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке Локальные адреса выберите одно из следующих значений:

- Любой адрес. Сетевое правило контролирует отправку и / или получение сетевых пакетов компьютерами с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и любым IP-адресом.
- Адреса из списка. Сетевое правило контролирует отправку и / или получение сетевых пакетов компьютерами с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и с IP-адресами, которые можно указать в списке ниже с помощью кнопок Добавить, Изменить и Удалить.

Иногда для программ, работающих с сетевыми пакетами, не удается получить локальный адрес. В этом случае значение параметра Локальные адреса игнорируется.

16. Установите флажок Записывать в отчет, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

17. Нажмите на кнопку OK в окне Сетевое правило.

Если вы создали новое сетевое правило, оно отобразится на закладке Сетевые пакетные правила окна Сетевой экран. По умолчанию новое сетевое правило помещается в конец списка сетевых пакетных правил.

18. Сохраните внесенные изменения.

Включение и выключение сетевого пакетного правила

Чтобы включить или выключить сетевое пакетное правило, выполните следующие действия:

1 В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.

3. Нажмите на кнопку Сетевые пакетные правила.

   Откроется окно Сетевой экран на закладке Сетевые пакетные правила.

4. Выберите в списке нужное сетевое пакетное правило.

5. Выполните одно из следующих действий:

   - Установите флажок рядом с названием сетевого пакетного правила, если вы хотите включить правило.
   - Снимите флажок рядом с названием сетевого пакетного правила, если вы хотите выключить правило.

6. Сохраните внесенные изменения.

Изменение действия Сетевого экрана для сетевого пакетного правила

Чтобы изменить действие Сетевого экрана для сетевого пакетного правила, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.

3. Нажмите на кнопку Сетевые пакетные правила.

   Откроется окно Сетевой экран на закладке Сетевые пакетные правила.

4. Выберите в списке сетевое пакетное правило, для которого вы хотите изменить действие.

5. В графе Разрешение по правой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - Разрешать.
   - Запрещать.
   - По правилу программы.
   - Записывать в отчет.

6. Сохраните внесенные изменения.

Изменение приоритета сетевого пакетного правила

Приоритет выполнения сетевого пакетного правила определяется его положением в списке сетевых пакетных правил. Первое сетевое пакетное правило в списке сетевых пакетных правил обладает самым высоким приоритетом.

Каждое сетевое пакетное правило, которое вы создали вручную, добавляется в конец списка сетевых пакетных правил и имеет самый низкий приоритет.

Сетевой экран выполняет правила в порядке их расположения в списке сетевых пакетных правил, сверху вниз. Согласно каждому обрабатываемому сетевому пакетному правилу, применяемому к определенному сетевому соединению, Сетевой экран либо разрешает, либо блокирует сетевой доступ к адресу и порту, указанным в настройках этого сетевого соединения.

Чтобы изменить приоритет сетевого пакетного правила, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.
3. Нажмите на кнопку Сетевые пакетные правила.

   Откроется окно Сетевой экран на закладке Сетевые пакетные правила.
4. Выберите в списке сетевое пакетное правило, приоритет которого вы хотите изменить.
5. С помощью кнопок Вверх и Вниз переместите сетевое пакетное правило на нужную позицию в списке сетевых пакетных правил.
6. Сохраните внесенные изменения.

Работа с сетевыми правилами программ

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready по умолчанию группирует все программы, установленные на компьютере пользователя, по названию производителей программного обеспечения, файловую и сетевую активность которого он контролирует. Группы программ, в свою очередь, сгруппированы в группы доверия. Все программы и группы программ наследуют свойства своей родительской группы: правила контроля программ, сетевые правила программы, а также приоритет их выполнения.

Как и компонент Предотвращение вторжений, компонент Сетевой экран по умолчанию применяет сетевые правила группы программ для фильтрации сетевой активности всех помещенных в группу программ. Сетевые правила группы программ определяют, какими правами доступа к различным сетевым соединениям обладают программы, входящие в эту группу.

Сетевой экран по умолчанию создает набор сетевых правил для каждой группы программ, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обнаружил на компьютере. Вы можете изменить действие Сетевого экрана для сетевых правил группы программ, созданных по умолчанию. Вы не можете изменить, удалить или выключить сетевые правила группы программ, созданные по умолчанию, а также изменить их приоритет.

Вы также можете создать сетевое правило для отдельной программы. Такое правило будет иметь более высокий приоритет, чем сетевое правило группы, в которую входит эта программа.

Вы можете выполнить следующие действия в процессе работы с сетевыми правилами программ:

- Создать новое сетевое правило.

.

Вы можете создать новое сетевое правило, в соответствии с которым Сетевой экран должен регулировать сетевую активность программы или программ, входящих в выбранную группу программ.

- Включить и выключить сетевое правило.

  Все сетевые правила добавляются в список сетевых правил программ со статусом Включено. Если сетевое правило включено, Сетевой экран применяет это правило.

  Вы можете выключить сетевое правило, созданное вручную. Если сетевое правило выключено, Сетевой экран временно не применяет это правило.

- Изменить параметры сетевого правила.

  После того как вы создали новое сетевое правило, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Изменить действие Сетевого экрана для сетевого правила.

  В списке сетевых правил вы можете изменить действие для сетевого правила, которое Сетевой экран выполняет, обнаружив сетевую активность этой программы или группы программ.

- Изменить приоритет сетевого правила.

  Вы можете повысить или понизить приоритет созданного вручную сетевого правила.

- Удалить сетевое правило.

  Вы можете удалить созданное вручную сетевое правило, если вы не хотите, чтобы Сетевой экран применял это сетевое правило к выбранной программе или группе программ при обнаружении сетевой активности, и чтобы оно отображалось в списке сетевых правил программ.

Создание и изменение сетевого правила программ

Чтобы создать или изменить сетевое правило программы или группы программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.
3. Нажмите на кнопку Правила программ.

   Откроется окно Сетевой экран на закладке Сетевые правила программ.
4. В списке программ выберите программу или группу программ, для которой вы хотите создать или изменить сетевое правило.
5. По правой клавише мыши откройте контекстное меню и в зависимости от того, что вам нужно сделать, выберите пункт Права программы или Права группы.

   Откроется окно Права программы или Права группы программ.
6. Выберите закладку Сетевые правила в окне Права программы или Права группы программ.
7. Выполните одно из следующих действий:

- Если хотите создать новое сетевое правило, нажмите на кнопку Добавить.
- Если хотите изменить сетевое правило, выберите его в списке сетевых правил и нажмите на кнопку Изменить.

Откроется окно Сетевое правило.

8 В раскрывающемся списке Действие выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:

- Разрешать.
- Запрещать.

9. В поле Название укажите название сетевой службы одним из следующих способов:

- Нажмите на значок , расположенный справа от поля Название, и в раскрывающемся списке выберите название сетевой службы.

  В раскрывающийся список входят сетевые службы, описывающие наиболее часто используемые сетевые соединения.

- В поле Название введите название сетевой службы вручную.

10. Укажите протокол передачи данных:

a. Установите флажок Протокол.

b. В раскрывающемся списке выберите тип протокола, по которому должен производиться контроль сетевой активности.

Сетевой экран контролирует соединения по протоколам TCP, UDP, ICMP, ICMPv6, IGMP и GRE. Если сетевая служба выбрана в раскрывающемся списке Название, то флажок Протокол устанавливается автоматически и в раскрывающемся списке рядом с флажком выбирается тип протокола, который соответствует выбранной сетевой службе. По умолчанию флажок Протокол снят.

11. В раскрывающемся списке Направление выберите направление контролируемой сетевой активности.

Сетевой экран контролирует сетевые соединения со следующими направлениями:

- Входящее.
- Входящее / Исходящее.
- Исходящее.

12. Если в качестве протокола выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета:

a. Установите флажок ICMP-тип и в раскрывающемся списке выберите тип ICMP-пакета.

b. Установите флажок ICMP-код и в раскрывающемся списке выберите код ICMP-пакета.

13. Если в качестве протокола выбран протокол TCP или UDP, вы можете через запятую указать номера портов компьютера пользователя и удаленного компьютера, соединение между которыми следует контролировать:

    a. В поле Удаленные порты введите порты удаленного компьютера.

    b. В поле Локальные порты введите порты компьютера пользователя.

14. Укажите сетевые адреса удаленных компьютеров, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке Удаленные адреса выберите одно из следующих значений:

    - Любой адрес. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.
    - Адреса подсети. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, относящимися к выбранному типу сети: Доверенные сети, Локальные сети, Публичные сети.
    - Адреса из списка. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, которые можно указать в списке ниже с помощью кнопок Добавить, Изменить и Удалить.

15. Укажите сетевые адреса компьютеров с установленной программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке Локальные адреса выберите одно из следующих значений:

    - Любой адрес. Сетевое правило контролирует отправку и / или получение сетевых пакетов компьютерами с установленной программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и любым IP-адресом.
    - Адреса из списка. Сетевое правило контролирует отправку и / или получение сетевых пакетов компьютерами с установленной программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и с IP-адресами, которые можно указать в списке ниже с помощью кнопок Добавить, Изменить и Удалить.

    Иногда для программ, работающих с сетевыми пакетами, не удается получить локальный адрес. В этом случае значение параметра Локальные адреса игнорируется.

16. Установите флажок Записывать в отчет, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

17. Нажмите на кнопку OK в окне Сетевое правило.

    Если вы создали новое сетевое правило, оно отобразится на закладке Сетевые правила.

18. Нажмите на кнопку OK в окне Права группы программ, если правило предназначено для группы программ, или в окне Права программы, если правило предназначено для программы.

19. Сохраните внесенные изменения.

Включение и выключение сетевого правила программ

Чтобы включить или выключить сетевое правило программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.
3. Нажмите на кнопку Правила программ.

   Откроется окно Сетевой экран на закладке Сетевые правила программ.
4. В списке выберите программу или группу программ, для которой вы хотите включить или выключить сетевое правило.
5. По правой клавише мыши откройте контекстное меню и в зависимости от того, что вам нужно сделать, выберите пункт Права программы или Права группы.

   Откроется окно Права программы или Права группы программ.
6. В открывшемся окне выберите закладку Сетевые правила.

7 В списке сетевых правил группы программ выберите нужное вам сетевое правило.

8. Выполните одно из следующих действий:
   - Установите флажок рядом с названием сетевого правила, если вы хотите включить правило.
   - Снимите флажок рядом с названием сетевого правила, если вы хотите выключить правило.

   Вы не можете выключить сетевое правило группы программ, если оно создано Сетевым экраном по умолчанию.
9. Нажмите на кнопку OK в окне Права группы программ, если правило предназначено для группы программ, или в окне Права программы, если правило предназначено для программы.
10. Сохраните внесенные изменения.

Изменение действия Сетевого экрана для сетевого правила программ

Вы можете изменить действие Сетевого экрана для всех сетевых правил программы или группы программ, которые были созданы по умолчанию, а также изменить действие Сетевого экрана для одного сетевого правила программы или группы программ, которое было создано вручную.

Чтобы изменить действие Сетевого экрана для всех сетевых правил программы или группы программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.

.

3. Нажмите на кнопку Правила программ.

   Откроется окно Сетевой экран на закладке Сетевые правила программ.

4. В списке выберите программу или группу программ, если вы хотите изменить действие Сетевого экрана для всех ее сетевых правил, созданных по умолчанию. Сетевые правила, созданные вручную, останутся без изменений.

5. В графе Сеть по левой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - Наследовать.
   - Разрешать.
   - Запрещать.

6. Сохраните внесенные изменения.

Чтобы изменить действие Сетевого экрана для одного сетевого правила программы или группы программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2 В окне параметров программы выберите раздел Базовая защита → Сетевой экран.

3. Нажмите на кнопку Правила программ.

   Откроется окно Сетевой экран на закладке Сетевые правила программ.

4. В списке выберите программу или группу программ, для которой вы хотите изменить действие одного сетевого правила.

5. По правой клавише мыши откройте контекстное меню и в зависимости от того, что вам нужно сделать, выберите пункт Права программы или Права группы.

   Откроется окно Права программы или Права группы программ.

6. В открывшемся окне выберите закладку Сетевые правила.

7. Выберите сетевое правило, для которого вы хотите изменить действие Сетевого экрана.

8. В графе Разрешение по правой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - Разрешать.
   - Запрещать.
   - Записывать в отчет.

9. Нажмите на кнопку OK в окне Права группы программ, если правило предназначено для группы программ, или в окне Права программы, если правило предназначено для программы.

10. Сохраните внесенные изменения.

Изменение приоритета сетевого правила программ

Приоритет выполнения сетевого правила определяется его положением в списке сетевых правил. Сетевой экран выполняет правила в порядке их расположения в списке сетевых правил, сверху вниз. Согласно каждому обрабатываемому сетевому правилу, применяемому к определенному сетевому соединению, Сетевой экран либо разрешает, либо блокирует сетевой доступ к адресу и порту, указанным в настройках этого сетевого соединения.

Созданные вручную сетевые правила имеют более высокий приоритет, чем сетевые правила, созданные по умолчанию.

Вы не можете изменить приоритет сетевых правил группы программ, созданных по умолчанию.

Чтобы изменить приоритет сетевого правила, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Базовая защита → Сетевой экран.

3. Нажмите на кнопку Правила программ.

.

Откроется окно Сетевой экран на закладке Сетевые правила программ.

4 В списке программ выберите программу или группу программ, для которой вы хотите изменить приоритет сетевого правила.

5. По правой клавише мыши откройте контекстное меню и в зависимости от того, что вам нужно сделать, выберите пункт Права программы или Права группы.

   Откроется окно Права программы или Права группы программ.

6. В открывшемся окне выберите закладку Сетевые правила.

7. Выберите сетевое правило, приоритет которого вы хотите изменить.

8. С помощью кнопок Вверх и Вниз переместите сетевое правило на нужную позицию в списке сетевых правил.

9. Нажмите на кнопку ОК в окне Права группы программ, если правило предназначено для группы программ, или в окне Права программы, если правило предназначено для программы.

10. Сохраните внесенные изменения.

Мониторинг сети

Мониторинг сети – это инструмент, предназначенный для просмотра информации о сетевой активности компьютера пользователя в реальном времени.

Чтобы запустить мониторинг сети, выполните следующие действия:

1. В главном окне программы нажмите на блок Компоненты защиты.

2. Нажмите на ссылку Мониторинг сети в нижней части окна.

   Откроется окно Мониторинг сети. В этом окне информация о сетевой активности компьютера пользователя представлена на четырех закладках:

   - На закладке Сетевая активность отображаются все активные на текущий момент сетевые соединения с компьютером пользователя. Приводятся как сетевые соединения, инициированные компьютером пользователя, так и входящие сетевые соединения.
   - На закладке Открытые порты перечислены все открытые сетевые порты на компьютере пользователя.
   - На закладке Сетевой трафик отображается объем входящего и исходящего сетевого трафика между компьютером пользователя и другими компьютерами сети, в которой пользователь работает в текущий момент.
   - На закладке Заблокированные компьютеры представлен список IP-адресов удаленных компьютеров, сетевую активность которых компонент Защита от сетевых угроз заблокировал, обнаружив попытку сетевой атаки с этого IP-адреса.

Защита от атак BadUSB

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру.

Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USBустройств, имитирующих клавиатуру.

Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, программа предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный программой. Эта процедура называется авторизацией клавиатуры. Программа разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

Компонент Защита от атак BadUSB не устанавливается по умолчанию. Если вам нужен компонент Защита от атак BadUSB, вы можете добавить компонент в свойствах инсталляционного пакета перед установкой программы или измените состав компонентов программы после установки программы.

Включение и выключение Защиты от атак BadUSB

Чтобы включить или выключить Защиту от атак BadUSB, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от атак BadUSB.
3. Выполните одно из следующих действий:
   - Установите флажок Защита от атак BadUSB, если вы хотите включить Защиту от атак BadUSB.
   - Снимите флажок Защита от атак BadUSB, если вы хотите выключить Защиту от атак BadUSB.
4. Сохраните внесенные изменения.

Разрешение и запрещение использования экранной клавиатуры при авторизации

Возможность использовать экранную клавиатуру предназначена только для авторизации USB-устройств, не поддерживающих произвольный ввод символов (например, сканеров штрих-кодов). Не рекомендуется использовать экранную клавиатуру для авторизации неизвестных вам USB-устройств.

Чтобы разрешить или запретить использование экранной клавиатуры при авторизации, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Защита от атак BadUSB.

   В правой части окна отобразятся параметры компонента.

.

3. Выполните одно из следующих действий:

   - Установите флажок Запретить использование экранной клавиатуры для авторизации USBустройств, если вы хотите запретить использование экранной клавиатуры для авторизации.

   - Снимите флажок Запретить использование экранной клавиатуры для авторизации USB-устройств, если вы хотите разрешить использование экранной клавиатуры для авторизации.

4 Сохраните внесенные изменения.

Авторизация клавиатуры

USB-устройства, определенные операционной системой как клавиатуры и подключенные к компьютеру до установки компонента Защита от атак BadUSB, считаются авторизованными после его установки.

Программа требует авторизацию подключенного USB-устройства, определенного операционной системой как клавиатура, если включен запрос авторизации USB-клавиатур. Пользователь не может использовать неавторизованную клавиатуру до тех пор, пока она не будет авторизована.

Если запрос авторизации USB-клавиатур выключен, пользователь может использовать все подключенные клавиатуры. Сразу после включения запроса авторизации USB-клавиатур программа запрашивает авторизацию для каждой подключенной неавторизованной клавиатуры.

Чтобы авторизовать клавиатуру, выполните следующие действия:

1. При включенной авторизации USB-клавиатур подключите клавиатуру к USB-порту.

   Откроется окно Авторизация клавиатуры <Название клавиатуры> с информацией о подключенной клавиатуре и цифровым кодом для ее авторизации.

2. С подключенной или экранной клавиатуры, если она доступна, последовательно введите случайно сформированной в окне авторизации цифровой код.

3. Нажмите на кнопку OK.

   Если код введен правильно, программа сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

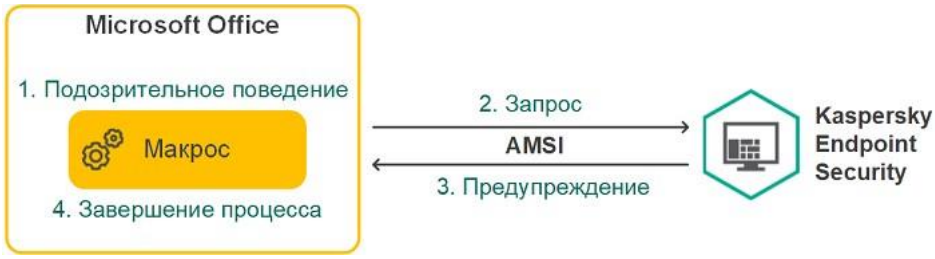
   > При подключении авторизованной клавиатуры через другой USB-порт компьютера программа снова запрашивает ее авторизацию.

   Если цифровой код введен неправильно, программа формирует новый. Число попыток для ввода цифрового кода равно трем. Если цифровой код введен неправильно трижды или закрыто окно Авторизация клавиатуры <Название клавиатуры>, программа блокирует ввод с этой клавиатуры. При повторном подключении клавиатуры или перезагрузке операционной системы программа снова предлагает пройти авторизацию клавиатуры.

Поставщик AMSI-защиты

Поставщик AMSI-защиты предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft. Интерфейс Antimalware Scan Interface (AMSI) позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для дополнительной проверки и получать результаты проверки этих объектов. Сторонними приложениями могут быть, например, программы Microsoft O ice (см. рис. ниже). Подробнее об интерфейсе AMSI см. в документации Microsoft.

Поставщик AMSI-защиты может только обнаруживать угрозу и уведомлять стороннее приложение об обнаруженной угрозе. Стороннее приложение после получения уведомления об угрозе не дает выполнить вредоносные действия (например, завершает работу).



Пример работы AMSI

Компонент Поставщик AMSI-защиты может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправляет информацию об отклонении запроса от стороннего приложения на Сервер администрирования. Компонент Поставщик AMSI-защиты не отклоняет запросы от тех сторонних приложений, для которых установлен флажок Не блокировать взаимодействие с Поставщиком AMSIзащиты.

Поставщик AMSI-защиты доступен для следующих операционных систем рабочих станций и серверов:

- Windows 10 Home / Pro / Education / Enterprise;
- Windows Server 2016 Essentials / Standard /
- Datacenter; Windows Server 2019 Essentials /

Standard / Datacenter.

Включение и выключение Поставщика AMSI-защиты

По умолчанию Поставщик AMSI-защиты включен.

Чтобы включить или выключить Поставщик AMSI-защиты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Базовая защита → Поставщик AMSI-защиты.

.

3. Выполните одно из следующих действий:

   - Установите флажок Поставщик AMSI-защиты, если вы хотите включить Поставщик AMSI-защиты.
   - Снимите флажок Поставщик AMSI-защиты, если вы хотите выключить Поставщик AMSI-защиты.

4. Сохраните внесенные изменения.

Проверка составных файлов Поставщиком AMSI-защиты

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы. Чтобы обнаружить скрытые таким образом вирусы и другие программы, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить набор типов проверяемых составных файлов, таким образом увеличив скорость проверки.

Чтобы настроить проверку составных файлов Поставщиком AMSI-защиты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Поставщик AMSI-защиты.
3. В блоке Проверка составных файлов укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.
4. В блоке Ограничение по размеру выполните одно из следующих действий:
   - Чтобы запретить компоненту Поставщик AMSI-защиты распаковывать составные файлы большого размера, установите флажок Не распаковывать составные файлы большого размера и в поле Максимальный размер файла укажите нужное значение. Компонент Поставщик AMSI-защиты не будет распаковывать составные файлы больше указанного размера.
   - Чтобы разрешить компоненту Поставщик AMSI-защиты распаковывать составные файлы большого размера, снимите флажок Не распаковывать составные файлы большого размера.

   Компонент Поставщик AMSI-защиты проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок Не распаковывать составные файлы большого размера.
5. Сохраните внесенные изменения.

Контроль компьютера

Контроль программ

Контроль программ управляет запуском программ на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании программ. Также Контроль программ снижает риск заражения компьютера, ограничивая доступ к программам.

Настройка Контроля программ состоит из следующих этапов:

1. Создание категорий программ.

   Администратор создает категории программ, которыми администратор хочет управлять. Категории программ предназначены для всех компьютеров сети организации независимо от групп администрирования. Для создания категории вы можете использовать следующие критерии: KL-категория (например, Браузеры), хеш файла, производитель программы и другие.

2. Создание правил Контроля программ.

   Администратор создает правила Контроля программ в политике для группы администрирования. Правило включает в себя категории программ и статус запуска программ из этих категорий: запрещен или разрешен.

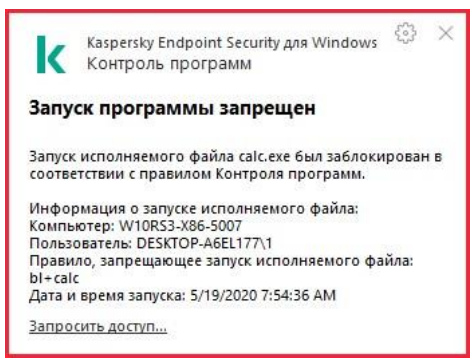
3. Выбор режима работы Контроля программ.

   Администратор выбирает режим работы с программами, которые не входят ни в одно из правил: черный и белый списки.

При попытке пользователя запустить запрещенную программу, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует запуск программы и покажет уведомление (см. рис. ниже).

Для проверки настройки Контроля программ предусмотрен тестовый режим. В этом режиме Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

- разрешает запуск программ, в том числе запрещенных;
- показывает уведомление о запуске запрещенной программы и добавляет информацию в отчет на компьютере пользователя; • отправляет данные о запуске запрещенных программ в Kaspersky Security Center.



Уведомление Контроля программ

Режимы работы Контроля программ

Компонент Контроль программ может работать в двух режимах:

- Черный список. Режим, при котором Контроль программ разрешает пользователям запуск любых программ, кроме тех, которые запрещены в правилах Контроля программ.

  Этот режим работы Контроля программ установлен по умолчанию.

- Белый список. Режим, при котором Контроль программ запрещает пользователям запуск любых программ, кроме тех, которые разрешены и не запрещены в правилах Контроля программ.

  Если разрешающие правила Контроля программ сформированы максимально полно, компонент запрещает запуск всех новых программ, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

  Вы можете ознакомиться с рекомендациями по настройке правил контроля программ в режиме белого списка.

Настройка Контроля программ для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, так и с помощью Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и необходимые для следующих задач:

- Создание категорий программ.

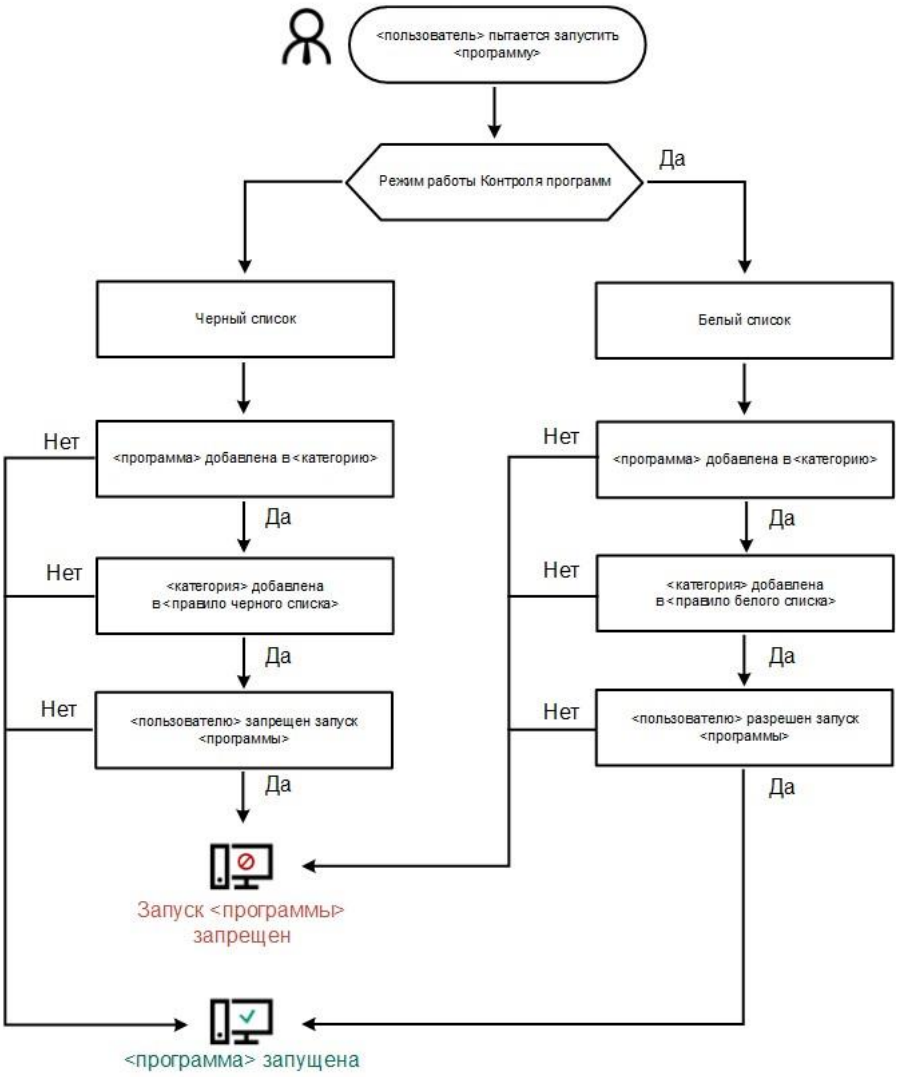
  Правила Контроля программ, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях программ, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

- Получение информации о программах, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль программ рекомендуется выполнять с помощью Kaspersky Security Center.

Алгоритм работы Контроля программ

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует алгоритм для принятия решения о запуске программы (см. рис. ниже).



Алгоритм работы Контроля программ

Ограничения функциональности Контроля программ

Работа компонента Контроль программ ограничена в следующих случаях:

- При обновлении версии программы импорт параметров компонента Контроль программ не поддерживается.
- При обновлении версии программы импорт параметров компонента Контроль программ поддерживается только при обновлении версии Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows и выше до Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11.4.0 для Windows.

При обновлении версий программы, отличных от Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows, для восстановления работоспособности Контроля программ необходимо заново настроить параметры работы компонента.

- При отсутствии соединения с серверами KSN Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready получает информацию о репутации программ и их модулей только из локальных баз.

  Список программ, для которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready определяет KL-категорию Программы, доверенные согласно репутации в KSN, при наличии соединения с серверами KSN может отличаться от списка программ, для которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready определяет KL-категорию Программы, доверенные согласно репутации в KSN, при отсутствии соединения с KSN.

- В базе данных Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого количества записей новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с компьютера, на котором установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

- Компонент не контролирует запуск скриптов, если скрипт передается интерпретатору не через командную строку.

  Если запуск интерпретатора разрешен правилами Контроля программ, то компонент не блокирует скрипт, запущенный из этого интерпретатора.

  Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля программ, то компонент блокирует все скрипты, указанные в командной строке интерпретатора.

- Компонент не контролирует запуск скриптов из интерпретаторов, не поддерживаемых программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает следующие интерпретаторы:

  - Java;
  - PowerShell.

  Поддерживаются следующие типы интерпретаторов:

- %ComSpec%;
- %SystemRoot%\\system32\\regedit.exe;
- %SystemRoot%\\regedit.exe;
- %SystemRoot%\\system32\\regedt32.exe;
- %SystemRoot%\\system32\\cscript.exe;
- %SystemRoot%\\system32\\wscript.exe;
- %SystemRoot%\\system32\\msiexec.exe;
- %SystemRoot%\\system32\\mshta.exe;
- %SystemRoot%\\system32\\rundll32.exe;
- %SystemRoot%\\system32\\wwahost.exe;
- %SystemRoot%\\syswow64\\cmd.exe;
- %SystemRoot%\\syswow64\\regedit.exe;
- %SystemRoot%\\syswow64\\regedt32.exe;
- %SystemRoot%\\syswow64\\cscript.exe;
- %SystemRoot%\\syswow64\\wscript.exe;
- %SystemRoot%\\syswow64\\msiexec.exe;
- %SystemRoot%\\syswow64\\mshta.exe;
- %SystemRoot%\\syswow64\\rundll32.exe;
- %SystemRoot%\\syswow64\\wwahost.exe.

Включение и выключение Контроля программ

По умолчанию Контроль программ выключен.

Чтобы включить или выключить Контроль программ выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль программ.
3. Выполните одно из следующих действий:

- Установите флажок Контроль программ, если вы хотите включить Контроль программ.
- Снимите флажок Контроль программ, если вы хотите выключить Контроль программ.

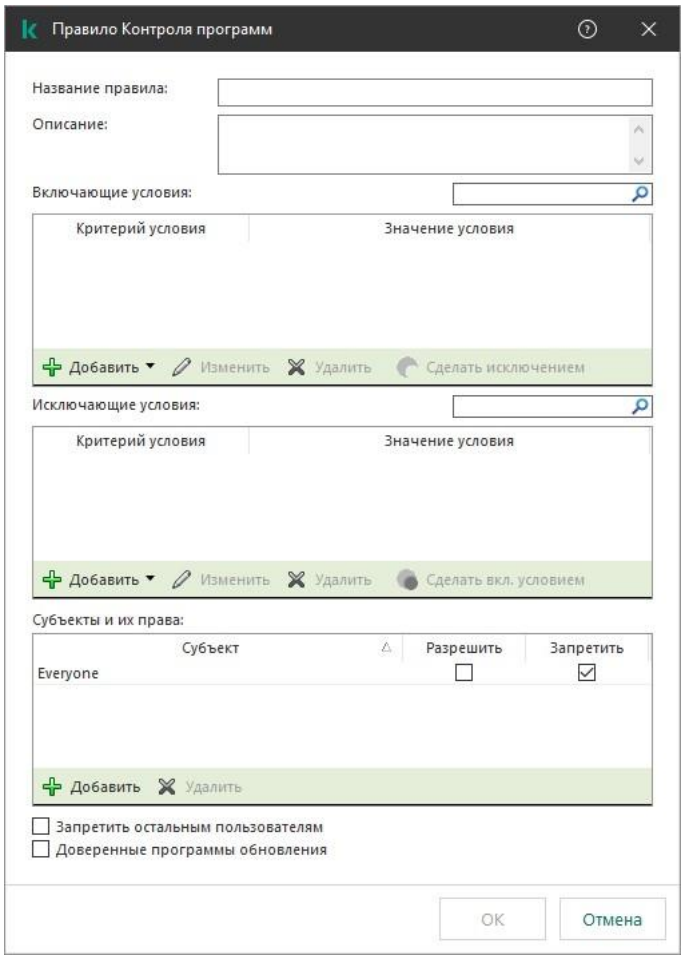
4. Сохраните внесенные изменения.

Управление правилами Контроля программ

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует запуск программ пользователями с помощью правил. В правиле Контроля программ содержатся условия срабатывания и действия компонента Контроль программ при срабатывании правила (разрешение или запрещение пользователям запускать программу).

Условия срабатывания правила

Условие срабатывания правила представляет собой соответствие "тип условия - критерий условия значение условия" (см. рис. ниже). На основании условий срабатывания правила Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready применяет (или не применяет) правило к программе.



Правило Контроля программ. Параметры условий срабатывания правила

В правилах используются включающие и исключающие условия:

- Включающие условия. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready применяет правило к программе, если программа соответствует хотя бы одному включающему условию.

- Исключающие условия. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не применяет правило к программе, если программа соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию.

Условия срабатывания правила формируются с помощью критериев. Для формирования условий в Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready используются следующие критерии:

- путь к папке с исполняемым файлом программы или путь к исполняемому файлу программы;
- метаданные: название исполняемого файла программы, версия исполняемого файла программы, название программы, версия программы, производитель программы; хеш исполняемого файла программы; сертификат: издатель, субъект, отпечаток; принадлежность программы к KL-категории;
- расположение исполняемого файла программы на съемном диске.
- Для каждого критерия, используемого в условии, нужно указать его значение. Если параметры запускаемой программы соответствуют значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль программ выполняет действие, прописанное в правиле. Если параметры программы соответствуют значениям критериев, указанных в исключающем условии, Контроль программ не контролирует запуск программы.

Решения компонента Контроль программ при срабатывании правила

При срабатывании правила Контроль программ в соответствии с правилом разрешает или запрещает пользователям (группам пользователей) запускать программы. Вы можете выбирать отдельных пользователей или группы пользователей, которым разрешен или запрещен запуск программ, для которых срабатывает правило.

Если в правиле не указан ни один пользователь, которому разрешен запуск программ, удовлетворяющих правилу, правило называется запрещающим.

Если в правиле не указан ни один пользователь, которому запрещен запуск программ, удовлетворяющих правилу, правило называется разрешающим.

Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей назначено разрешающее правило Контроля программы и для одного из пользователей этой группы назначено запрещающее правило Контроля программы, то этому пользователю будет запрещен запуск программы.

Статус работы правила

Правила Контроля программ могут иметь один из следующих статусов работы:

- Вкл. Статус означает, что правило используется во время работы компонента Контроль программ.
- Выкл. Статус означает, что правило не используется во время работы компонента Контроль программ.

Тест. Статус означает, что Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает запуск программ, на которые распространяется действие правила, но заносит информацию о запуске этих программ в отчет.

Получение информации о программах, которые установлены на компьютерах пользователей

Для создания оптимальных правил Контроля программ рекомендуется получить представление о программах, используемых на компьютерах локальной сети организации. Для этого вы можете получить следующую информацию:

- производители, версии и локализации программ, которые используются в локальной сети
- организации; регулярность обновлений программ;
- политики использования программ, принятые в организации (это могут быть политики безопасности или административные политики); • расположение хранилища дистрибутивов программ.

Чтобы получить информацию о программах, которые используются на компьютерах локальной сети организации, вы можете использовать данные, представленные в папках Реестр программ и Исполняемые файлы. Папки Реестр программ и Исполняемые файлы входят в состав папки Управление программами дерева Консоли администрирования Kaspersky Security Center.

Папка Реестр программ содержит список программ, которые обнаружил на клиентских компьютерах установленный на них Агент администрирования.

Папка Исполняемые файлы содержит список исполняемых файлов, которые когда-либо запускались на клиентских компьютерах или были обнаружены в процессе работы задачи инвентаризации для Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Открыв окно свойств выбранной программы в папке Реестр программ или Исполняемые файлы, вы можете получить общую информацию о программе и о ее исполняемых файлах, а также просмотреть список компьютеров, на которых установлена эта программа.

Чтобы открыть окно свойств программы в папке Реестр программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите Дополнительно → Управление программами → Реестр программ.
3. Выберите программу.
4. В контекстном меню программы выберите пункт Свойства.

Чтобы открыть окно свойств исполняемого файла в папке Исполняемые файлы, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве Консоли администрирования выберите папку Дополнительно → Управление программами → Исполняемые файлы.

3. Выберите исполняемый файл.

4. В контекстном меню исполняемого файла выберите пункт Свойства.

Создание категорий программ

Для удобства формирования правил Контроля программ вы можете создать категории программ.

Рекомендуется создать категорию "Программы для работы", которая включает в себя стандартный набор программ, используемых в организации. Если различные группы пользователей используют различные наборы программ для работы, вы можете создать отдельную категорию программ для работы каждой группы пользователей.

Чтобы создать категорию программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве Консоли администрирования выберите папку Дополнительно → Управление программами → Категории программ.

3. В рабочей области нажмите на кнопку Создать категорию.

   Запустится мастер создания пользовательской категории.

4. Следуйте указаниям мастера создания пользовательской категории.

Шаг 1. Выбор типа категории

На этом шаге выберите один из следующих типов категорий программ:

- Пополняемая вручную категория. Если вы выбрали этот тип категории, то на шаге "Настройка условий для включения программ в категорию" и шаге "Настройка условий для исключения программ из категории" вы сможете задать критерии, по которым исполняемые файлы будут попадать в категорию.

- Категория, в которую входят исполняемые файлы с выбранных устройств. Если вы выбрали этот тип категории, то на шаге "Параметры" вы сможете указать компьютер, исполняемые файлы с которого будут автоматически попадать в категорию.

- Категория, в которую входят исполняемые файлы из указанной папки. Если вы выбрали этот тип категории, то на шаге "Папка хранилища" вы сможете указать папку, исполняемые файлы из которой будут автоматически попадать в категорию.

При создании автоматически пополняемой категории Kaspersky Security Center выполняет инвентаризацию файлов следующих форматов: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR.

Шаг 2. Ввод названия пользовательской

категории На этом шаге укажите название категории

программ.

Шаг 3. Настройка условий для включения программ в категорию

Этот шаг доступен, если вы выбрали тип категории Пополняемая вручную категория.

На этом шаге в раскрывающемся списке Добавить выберите условия для включения программ в категорию:

- Из списка исполняемых файлов. Добавьте программы из списка исполняемых файлов на клиентском устройстве в пользовательскую категорию.
- Из свойств файла. Укажите детальные данные исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.
- Метаданные файлов папки. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет метаданные этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.
- Хеши файлов папки. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет хеши этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.

- Сертификаты файлов из папки. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Kaspersky Security Center укажет сертификаты этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.

  Не рекомендуется использовать условия, в свойствах которых не указывается параметр Отпечаток сертификата.

- Метаданные файлов установщика MSI. Выберите MSI-пакет. Kaspersky Security Center укажет метаданные исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления программ в пользовательскую категорию.

- Контрольные суммы файлов msi-инсталлятора программы. Выберите MSI-пакет. Kaspersky Security Center укажет хеши исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления программ в пользовательскую категорию.

- KL-категория. Укажите KL-категорию в качестве условия добавления программ в пользовательскую категорию. KL-категория – сформированный специалистами "Лаборатории Касперского" список программ, обладающих общими тематическими признаками. Например, KL-категория "Офисные программы" включает в себя программы из пакетов Microsoft O ice, Adobe Acrobat и другие.

  Вы можете выбрать все KL-категории, чтобы сформировать расширенный список доверенных программ.

- Папка программы. Выберите папку на клиентском устройстве. Kaspersky Security Center добавит исполняемые файлы из этой папки в пользовательскую категорию.

- Сертификаты из хранилища сертификатов. Выберите сертификаты, которыми подписаны исполняемые файлы, в качестве условия добавления программ в пользовательскую категорию.

  Не рекомендуется использовать условия, в свойствах которых не указывается параметр Отпечаток сертификата.

- Тип носителя. Укажите тип запоминающего устройства (все жесткие и съемные диски или только съемные диски) в качестве условия добавления программ в пользовательскую категорию.

Шаг 4. Настройка условий для исключения программ из категории

Этот шаг доступен, если вы выбрали тип категории Пополняемая вручную категория.

Программы, указанные на этом шаге, исключаются из категории, даже если эти программы были указаны на шаге "Настройка условий для включения программ в категорию".

На этом шаге в раскрывающемся списке Добавить выберите условия для исключения программ из категории:

- Из списка исполняемых файлов. Добавьте программы из списка исполняемых файлов на клиентском устройстве в пользовательскую категорию.

-
- Из свойств файла. Укажите детальные данные исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.

  Метаданные файлов папки. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет метаданные этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.

- Хеши файлов папки. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет хеши этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.

- Сертификаты файлов из папки. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Kaspersky Security Center укажет сертификаты этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.

- Метаданные файлов установщика MSI. Выберите MSI-пакет. Kaspersky Security Center укажет метаданные исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления программ в пользовательскую категорию.

- Контрольные суммы файлов msi-инсталлятора программы. Выберите MSI-пакет. Kaspersky Security Center укажет хеши исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления программ в пользовательскую категорию.

- KL-категория. Укажите KL-категорию в качестве условия добавления программ в пользовательскую категорию. KL-категория – сформированный специалистами "Лаборатории Касперского" список программ, обладающих общими тематическими признаками. Например, KL-категория "Офисные программы" включает в себя программы из пакетов Microsoft O ice, Adobe Acrobat и другие.

  Вы можете выбрать все KL-категории, чтобы сформировать расширенный список доверенных программ.

- Папка программы. Выберите папку на клиентском устройстве. Kaspersky Security Center добавит исполняемые файлы из этой папки в пользовательскую категорию.

- Сертификаты из хранилища сертификатов. Выберите сертификаты, которыми подписаны исполняемые файлы, в качестве условия добавления программ в пользовательскую категорию.

- Тип носителя. Укажите тип запоминающего устройства (все жесткие и съемные диски или только съемные диски) в качестве условия добавления программ в пользовательскую категорию.

Шаг 5. Параметры

Этот шаг доступен, если вы выбрали тип категории Категория, в которую входят исполняемые файлы с выбранных устройств.

На этом шаге нажмите на кнопку Добавить и укажите компьютеры, исполняемые файлы с которых Kaspersky Security Center добавит в категорию программ. Kaspersky Security Center добавит в категорию программ все исполняемые файлы с указанных компьютеров, представленные в папке Исполняемые файлы.

Также на этом шаге вы можете настроить следующие параметры:

-
- Алгоритм вычисления хеш-функции программой Kaspersky Security Center. Для выбора алгоритма необходимо установить хотя бы один из следующих флажков:
  - Вычислять SHA-256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows и выше).
  - Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows).

  Флажок Синхронизация данных с хранилищем Сервера администрирования. Установите этот флажок, если вы хотите, чтобы Kaspersky Security Center периодически очищал категорию программ и добавлял в нее все исполняемые файлы с указанных компьютеров, представленные в папке Исполняемые файлы.

  Если флажок Синхронизация данных с хранилищем Сервера администрирования снят, то после создания категории программ Kaspersky Security Center не будет вносить в нее изменения.
- Поле Период проверки (ч). В поле вы можете указать период времени в часах, по истечении которого Kaspersky Security Center очищает категорию программ и добавляет в нее все исполняемые файлы с указанных компьютеров, представленные в папке Исполняемые файлы.

  Поле доступно, если установлен флажок Синхронизация данных с хранилищем Сервера администрирования.

Шаг 6. Папка хранилища

Этот шаг доступен, если вы выбрали тип категории Категория, в которую входят исполняемые файлы из указанной папки.

На этом шаге нажмите на кнопку Обзор и укажите папку, в которой Kaspersky Security Center будет выполнять поиск исполняемых файлов для автоматического добавления в категорию программ.

Также на этом шаге вы можете настроить следующие параметры:

- Флажок Включать в категорию динамически подключаемые библиотеки (DLL). Установите этот флажок, если вы хотите, чтобы в категорию программ включались динамически подключаемые библиотеки (файлы формата DLL).

  При включении файлов формата DLL в категорию программ возможно снижение производительности работы Kaspersky Security Center.
- Флажок Включать в категорию данные о скриптах. Установите этот флажок, если вы хотите, чтобы в категорию программ включались скрипты.

  При включении скриптов в категорию программ возможно снижение производительности работы Kaspersky Security Center.
- Алгоритм вычисления хеш-функции программой Kaspersky Security Center. Для выбора алгоритма необходимо установить хотя бы один из следующих флажков:

- Вычислять SHA-256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows и выше).
- Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows).

- Флажок Принудительно проверять папку на наличие изменений. Установите этот флажок, если вы хотите, чтобы Kaspersky Security Center периодически выполнял поиск исполняемых файлов в папке автоматического пополнения категории программ.

  Если флажок Принудительно проверять папку на наличие изменений снят, Kaspersky Security Center выполняет поиск исполняемых файлов в папке автоматического пополнения категории программ, только если в этой папке были изменены, добавлены или удалены файлы.

  Поле Период проверки (ч). В поле вы можете указать период времени в часах, по истечении которого Kaspersky Security Center выполняет поиск исполняемых файлов в папке автоматического пополнения категории программ.

  Поле доступно, если установлен флажок Принудительно проверять папку на наличие изменений.

Шаг 7. Создание пользовательской категории

Чтобы завершить работу мастера установки программы, нажмите на кнопку Готово.

Добавление в категорию программ исполняемых файлов из папки Исполняемые файлы

В папке Исполняемые файлы отображается список исполняемых файлов, обнаруженных на компьютерах. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready формирует список исполняемых файлов после выполнения задачи инвентаризации.

Чтобы добавить в категорию программ исполняемые файлы из папки Исполняемые файлы, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите Дополнительно → Управление программами → Исполняемые файлы.
3. В рабочей области выберите исполняемые файлы, которые вы хотите добавить в категорию программ.
4. По правой клавише мыши откройте контекстное меню для выбранных исполняемых файлов и выберите пункт Добавить в категорию.

   Откроется окно Выберите категорию программ.
5. В окне Выберите категорию программ выполните следующие действия:

   - В верхней части окна выберите один из следующих вариантов:

   - Создать категорию программ. Выберите этот вариант, если вы хотите создать новую категорию программ и добавить в нее исполняемые файлы.

- Добавить правила в указанную категорию. Выберите этот вариант, если вы хотите выбрать существующую категорию программ и добавить в нее исполняемые файлы.

- В блоке Тип правила выберите один из следующих вариантов:

  - Добавить в правила включения. Выберите этот вариант, если вы хотите создать условия, добавляющие исполняемые файлы в категорию программ.

  - Добавить в правила исключения. Выберите этот вариант, если вы хотите создать условия, исключающие исполняемые файлы из категории программ.

- В блоке Тип информации о файле выберите один из следующих вариантов:

  - Данные сертификата (или SHA-256 для файлов без сертификата).

  - Данные сертификата (файлы без сертификата пропускаются).

- Только SHA-256 (файлы без SHA-256 пропускаются).
- Только MD5 (для совместимости с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 1).

6. Нажмите на кнопку OK.

Добавление в категорию программ исполняемых файлов, связанных с событиями

Чтобы добавить в категорию программ исполняемые файлы, связанные с событиями Контроля программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле Сервер администрирования дерева Консоли администрирования выберите закладку События.
3. Выберите выборку событий о работе компонента Контроль программ (Просмотр событий по результатам работы компонента Контроль программ, Просмотр событий по результатам тестовой работы компонента Контроля программ) в раскрывающемся списке События выборки.
4. Нажмите на кнопку Запустить выборку.
5. Выберите события, в связи с которыми вы хотите добавить в категорию программ исполняемые файлы.
6. По правой клавише мыши откройте контекстное меню для выбранных событий и выберите пункт Добавить в категорию.

   Откроется окно Выберите категорию программ.
7. В окне Выберите категорию программ выполните следующие действия:
   - В верхней части окна выберите один из следующих вариантов:
     - Создать категорию программ. Выберите этот вариант, если вы хотите создать новую категорию программ и добавить в нее исполняемые файлы.
     - Добавить правила в указанную категорию. Выберите этот вариант, если вы хотите выбрать существующую категорию программ и добавить в нее исполняемые файлы.
   - В блоке Тип правила выберите один из следующих вариантов:
     - Добавить в правила включения. Выберите этот вариант, если вы хотите создать условия, добавляющие исполняемые файлы в категорию программ.
     - Добавить в правила исключения. Выберите этот вариант, если вы хотите создать условия, исключающие исполняемые файлы из категории программ.

- В блоке Тип информации о файле выберите один из следующих вариантов:
  - Данные сертификата (или SHA-256 для файлов без сертификата).
  - Данные сертификата (файлы без сертификата пропускаются).
  - Только SHA-256 (файлы без SHA-256 пропускаются).
  - Только MD5 (для совместимости с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 1).

8. Нажмите на кнопку OK.

Добавление и изменение правила Контроля программ с помощью Kaspersky Security Center

Чтобы добавить или изменить правило Контроля программ с помощью Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Контроль безопасности → Контроль программ.
   В правой части окна отобразятся параметры компонента Контроль программ.
6. Выполните одно из следующих действий:
   - Если вы хотите добавить правило, нажмите на кнопку Добавить.
   - Если вы хотите изменить существующее правило, выберите правило в списке и нажмите на кнопку Изменить.

   Откроется окно Правило Контроля программ.
7. Выполните одно из следующих действий:
   - Если вы хотите создать новую категорию, выполните следующие действия:

     a. Нажмите на кнопку Создать категорию.
        Запустится мастер создания пользовательской категории.

     b. Следуйте указаниям мастера создания пользовательской категории.

     c. Из раскрывающегося списка Категория выберите созданную категорию программ.

- Если вы хотите изменить существующую категорию, выполните следующие действия:

  a. Из раскрывающегося списка Категория выберите созданную категорию программ, которую вы хотите изменить.

  b. Нажмите на кнопку Свойства.

  Откроется окно Свойства: <Название категории>.

  c. Измените параметры выбранной категории программ.

  d. Нажмите на кнопку OK.

  e. Из раскрывающегося списка Категория выберите созданную категорию программ, на основе которой вы хотите создать правило.

8. В таблице Субъекты и их права нажмите на кнопку Добавить.

   Откроется стандартное окно Microsoft Windows Выбор: "Пользователи" или "Группы".

9. В окне Выбор: "Пользователи" или "Группы" задайте список пользователей и / или групп пользователей, для которых вы хотите настроить возможность запускать программы, принадлежащие к выбранной категории.

10. В таблице Субъекты и их права выполните следующие действия:

    - Если вы хотите разрешить пользователям и / или группам пользователей запуск программ, принадлежащих к выбранной категории, установите флажок Разрешить в нужных строках.

    - Если вы хотите запретить пользователям и / или группам пользователей запуск программ, принадлежащих к выбранной категории, установите флажок Запретить в нужных строках.

11. Установите флажок Запретить остальным пользователям, если вы хотите, чтобы программа запрещала запуск программ, принадлежащих к выбранной категории, всем пользователям, которые не указаны в графе Субъект и не входят в группы пользователей, указанные в графе Субъект.

12. Установите флажок Доверенные программы обновления, если вы хотите, чтобы программы, входящие в выбранную категорию программ, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready считал доверенными программами обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

    При миграции параметров Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready осуществляется также миграция списка исполняемых файлов, созданных доверенными программами обновления.

13. Нажмите на кнопку OK.

14. Нажмите на кнопку Применить в разделе Контроль программ окна свойств политики.

Изменение статуса правила Контроля программ с помощью Kaspersky Security Center

Чтобы изменить статус правила Контроля программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Контроль безопасности → Контроль программ.

   В правой части окна отобразятся параметры компонента Контроль программ.
6. В графе Статус по левой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:

   - Вкл. Статус означает, что правило используется во время работы компонента Контроль программ.
   - Выкл. Статус означает, что правило не используется во время работы компонента Контроль программ.
   - Тест. Статус означает, что Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready всегда разрешает запуск программ, на которые распространяется действие правила, но заносит информацию о запуске этих программ в отчет.

   > С помощью статуса Тест вы можете назначить действие, аналогичное элементу Тестировать правила, для части правил, при выбранном элементе Применять правила в раскрывающемся списке Действие.
7. Сохраните внесенные изменения.

Тестирование правил Контроля программ с помощью Kaspersky Security Center

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля программ и проанализировать их работу. При включении тестирования правил Контроля программ Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не будет блокировать программы, запуск которых запрещен Контролем программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

Для анализа работы правил Контроля программ требуется изучить события по результатам работы компонента Контроль программ, приходящие в Kaspersky Security Center. Если для всех программ, которые необходимы для работы пользователю компьютера, отсутствуют события о запрете запуска в

тестовом режиме, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами правил, создать дополнительные или удалить существующие правила.

По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает запуск всех программ, кроме программ, запрещенных правилами.

Чтобы включить или выключить тестирование правил Контроля программ в Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Контроль безопасности → Контроль программ.

   В правой части окна отобразятся параметры компонента Контроль программ.
6. В раскрывающемся списке Режим контроля выберите один из следующих элементов:
   - Черный список, если вы хотите разрешать запуск всех программ, кроме программ, запрещенных правилами.
   - Белый список, если вы хотите запрещать запуск всех программ, кроме программ, разрешенных правилами.
7. Выполните одно из следующих действий:
   - Если вы хотите включить тестирование правил Контроля программ, в раскрывающемся списке Действие выберите элемент Тестировать правила.
   - Если вы хотите включить Контроль программ для управления запуском программ на компьютерах пользователей, в раскрывающемся списке Действие выберите элемент Применять правила.
8. Сохраните внесенные изменения.

Просмотр событий по результатам тестовой работы компонента Контроля программ

Чтобы просмотреть приходящие на Kaspersky Security Center события по результатам тестовой работы компонента Контроль программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле Сервер администрирования дерева Консоли администрирования выберите закладку События.
3. Нажмите на кнопку Создать выборку.

Откроется окно Свойства: <Название выборки>.

4. Откройте раздел События.
5. Нажмите на кнопку Сбросить все.
6. В таблице События установите флажки Запуск программы запрещен в тестовом режиме и Запуск программы разрешен в тестовом режиме.
7. Нажмите на кнопку OK.
8. В раскрывающемся списке События выборки выберите созданную выборку.
9. Нажмите на кнопку Запустить выборку.

Просмотр отчета о запрещенных программах в тестовом режиме

Чтобы просмотреть отчет о запрещенных программах в тестовом режиме, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле Сервер администрирования дерева Консоли администрирования выберите закладку Отчеты.
3. Нажмите на кнопку Новый шаблон отчета.

   Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. На шаге Выбор типа шаблона отчета выберите Другое → Отчет о запрещенных программах в тестовом режиме.

   После завершения работы мастера создания шаблона отчета в таблице на закладке Отчеты появится новый шаблон отчета.
5. Запустите процесс формирования отчета, созданного на предыдущих шагах инструкции, одним из следующих способов:

   - В контекстном меню отчета выберите пункт Показать отчет.
   - Перейдите по ссылке Показать отчет, которая находится в правой части рабочей области Консоли администрирования.
   - Откройте отчет двойным щелчком мыши.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Просмотр событий по результатам работы компонента Контроль программ

Чтобы просмотреть приходящие в Kaspersky Security Center события по результатам работы компонента Контроль программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле Сервер администрирования дерева Консоли администрирования выберите закладку События.
3. Нажмите на кнопку Создать выборку.

   Откроется окно Свойства: <Название выборки>.
4. Откройте раздел События.
5. Нажмите на кнопку Сбросить все.
6. В таблице События установите флажок Запуск программы запрещен.
7. Нажмите на кнопку ОК.
8. В раскрывающемся списке События выборки выберите созданную выборку.
9. Нажмите на кнопку Запустить выборку.

Просмотр отчета о запрещенных программах

Чтобы просмотреть отчет о запрещенных программах, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле Сервер администрирования дерева Консоли администрирования выберите закладку Отчеты.
3. Нажмите на кнопку Новый шаблон отчета.

   Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. На шаге Выбор типа шаблона отчета выберите Другое → Отчет о запрещенных программах.

   После завершения работы мастера создания шаблона отчета в таблице на закладке Отчеты появится новый шаблон отчета.
5. Запустите процесс формирования отчета, созданного на предыдущих шагах инструкции, одним из следующих способов:

   - В контекстном меню отчета выберите пункт Показать отчет.
   - Перейдите по ссылке Показать отчет, которая находится в правой части рабочей области Консоли администрирования.
   - Откройте отчет двойным щелчком мыши.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Выбор режима Контроля программ

Чтобы выбрать режим Контроля программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль программ.
3. Установите флажок Контроль программ, чтобы параметры компонента стали доступными для изменения.
4. В раскрывающемся списке Режим контроля выберите один из следующих элементов:
   - Черный список, если вы хотите разрешать запуск всех программ, кроме программ, указанных в запрещающих правилах;
   - Белый список, если вы хотите запрещать запуск всех программ, кроме программ, указанных в разрешающих правилах.

   Для режима белого списка изначально задано правило Операционная система и ее компоненты, которое разрешает запуск программ, входящих в KL-категорию "Программы ОС", и правило Доверенные программы обновления, которое разрешает запуск программ, входящих в KLкатегорию "Доверенные программы обновления". В KL-категорию "Программы ОС" входят программы, обеспечивающие нормальную работу операционной системы. В KL-категорию "Доверенные программы обновления" входят программы обновления наиболее известных производителей программного обеспечения. Вы не можете удалить эти правила. Параметры этих правил недоступны для изменения. По умолчанию правило Операционная система и ее компоненты включено, а правило Доверенные программы обновления выключено. Запуск программ, соответствующих условиям срабатывания этих правил, разрешен всем пользователям.

   Все правила, сформированные при выбранном режиме, сохраняются после смены режима для возможности их повторного использования. Чтобы вернуться к использованию этих правил, достаточно выбрать нужный режим в раскрывающемся списке Режим контроля.
5. В раскрывающемся списке Действие выберите, какое действие компонент должен выполнять при попытке пользователя запустить программу, запрещенную правилами Контроля программ.
6. Установите флажок Контролировать DLL и драйверы, если вы хотите, чтобы программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролировала загрузку DLL-модулей при запуске пользователями программ.

   Информация о модуле и программе, загрузившей этот модуль, будет сохранена в отчет.

   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует только DLL-модули и драйверы, загруженные с момента установки флажка Контролировать DLL и драйверы. Перезагрузите компьютер после установки флажка Контролировать DLL и драйверы, если вы хотите, чтобы программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролировала все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

   При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в разделе Контроль программ включено правило по умолчанию Операционная система и ее компоненты или другое правило, которое содержит KL-категорию "Доверенные сертификаты" и обеспечивает

загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Правила Контроля программ, созданные на основе других KL-категорий (за исключением KL-категории "Доверенные сертификаты"), не применяются при контроле загрузки DLL-модулей и драйверов. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле Операционная система и ее компоненты может привести к нестабильности операционной системы.

Рекомендуется включить защиту паролем для настройки параметров программы, чтобы иметь возможность выключить запрещающие правила, блокирующие запуск критически важных DLLмодулей и драйверов, не изменяя при этом параметры политики Kaspersky Security Center.

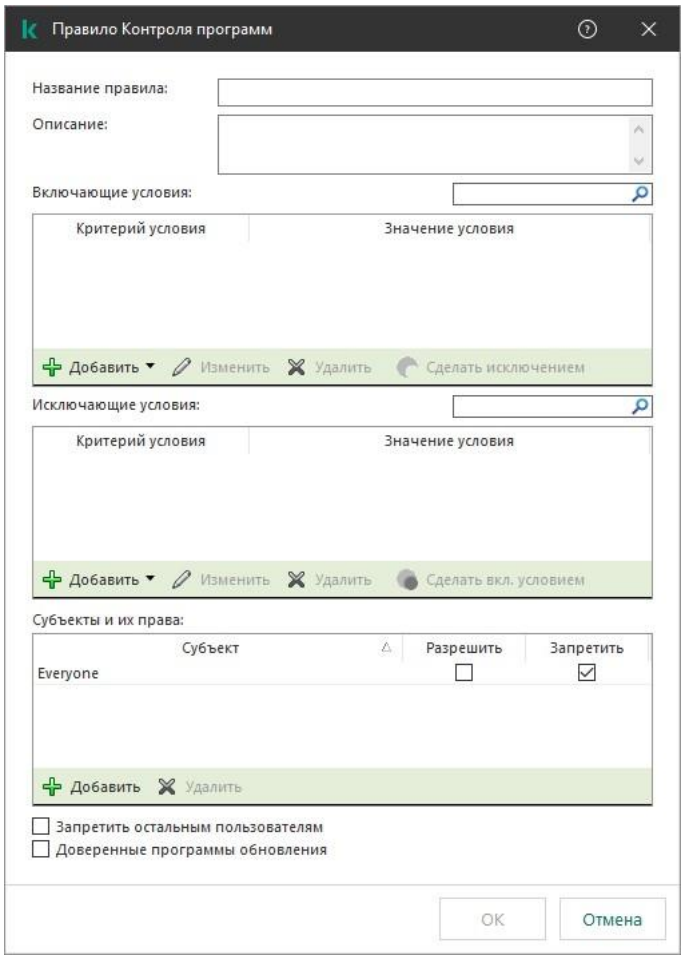
7. Сохраните внесенные изменения.

Действия с правилами Контроля программ

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует запуск программ пользователями с помощью правил. В правиле Контроля программ содержатся условия срабатывания и действия компонента Контроль программ при срабатывании правила (разрешение или запрещение пользователям запускать программу).

Условия срабатывания правила

Условие срабатывания правила представляет собой соответствие "тип условия - критерий условия значение условия" (см. рис. ниже). На основании условий срабатывания правила Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready применяет (или не применяет) правило к программе.



Правило Контроля программ. Параметры условий срабатывания правила

В правилах используются включающие и исключающие условия:

- Включающие условия. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready применяет правило к программе, если программа соответствует хотя бы одному включающему условию.
- Исключающие условия. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не применяет правило к программе, если программа соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию.

Условия срабатывания правила формируются с помощью критериев. Для формирования условий в Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready используются следующие критерии:

- путь к папке с исполняемым файлом программы или путь к исполняемому файлу программы;
- метаданные: название исполняемого файла программы, версия исполняемого файла программы, название программы, версия программы, производитель программы; хеш исполняемого файла программы; сертификат: издатель, субъект, отпечаток; принадлежность программы к KL-категории;
- расположение исполняемого файла программы на съемном диске.
- Для каждого критерия, используемого в условии, нужно указать его значение. Если параметры запускаемой программы соответствуют значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль программ выполняет действие, прописанное в правиле.

Если параметры программы соответствуют значениям критериев, указанных в исключающем условии, Контроль программ не контролирует запуск программы.

Решения компонента Контроль программ при срабатывании правила

При срабатывании правила Контроль программ в соответствии с правилом разрешает или запрещает пользователям (группам пользователей) запускать программы. Вы можете выбирать отдельных пользователей или группы пользователей, которым разрешен или запрещен запуск программ, для которых срабатывает правило.

Если в правиле не указан ни один пользователь, которому разрешен запуск программ, удовлетворяющих правилу, правило называется запрещающим.

Если в правиле не указан ни один пользователь, которому запрещен запуск программ, удовлетворяющих правилу, правило называется разрешающим.

Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей назначено разрешающее правило Контроля программы и для одного из пользователей этой группы назначено запрещающее правило Контроля программы, то этому пользователю будет запрещен запуск программы.

Статус работы правила

Правила Контроля программ могут иметь один из следующих статусов работы:

- Вкл. Статус означает, что правило используется во время работы компонента Контроль программ.
- Выкл. Статус означает, что правило не используется во время работы компонента Контроль программ.
- Тест. Статус означает, что Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает запуск программ, на которые распространяется действие правила, но заносит информацию о запуске этих программ в отчет.

Добавление и изменение правила Контроля программ

Чтобы добавить или изменить правило Контроля программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль программ.
3. Установите флажок Контроль программ, чтобы параметры компонента стали доступными для изменения.
4. Выполните одно из следующих действий:
   - Если вы хотите добавить правило, нажмите на кнопку Добавить.
   -

Если вы хотите изменить существующее правило, выберите правило в списке и нажмите на кнопку Изменить.

Откроется окно Правило Контроля программ.

5. Задайте или измените параметры правила:

   a. В поле Название правила введите или измените название правила.

   b. В таблице Включающие условия сформируйте или измените список включающих условий срабатывания правила с помощью кнопок Добавить, Изменить, Удалить, Сделать исключением.

   c. В таблице Исключающие условия сформируйте или измените список исключающих условий срабатывания правила с помощью кнопок Добавить, Изменить, Удалить, Сделать вкл. условием.

   d. Если требуется, измените тип условия срабатывания правила:

      - Чтобы сменить тип условия с включающего на исключающее, выберите условие в таблице Включающие условия и нажмите на кнопку Сделать исключением.

      - Чтобы сменить тип условия с исключающего на включающее, выберите условие в таблице Исключающие условия и нажмите на кнопку Сделать вкл. условием.

   e. Задайте или измените список пользователей и / или групп пользователей, которым разрешено или запрещено запускать программы, удовлетворяющие условиям срабатывания правила. Для этого нажмите на кнопку Добавить в таблице Субъекты и их права.

      По умолчанию в список пользователей добавлено значение Все. Действие правила распространяется на всех пользователей.

      Если в таблице не указан ни один пользователь, правило не может быть сохранено.

   f. В таблице Субъекты и их права установите флажки Разрешить или Запретить напротив пользователей и / или групп пользователей, чтобы определить их право на запуск программ.

      Флажок, установленный по умолчанию, зависит от режима работы Контроля программ.

   g. Установите флажок Запретить остальным пользователям, если вы хотите, чтобы программа запрещала запуск программ, удовлетворяющих условиям срабатывания правила, всем пользователям, которые не указаны в графе Субъект и не входят в группы пользователей, указанные в графе Субъект.

      Если флажок Запретить остальным пользователям снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не контролирует запуск программ пользователями, которые не указаны в таблице Субъекты и их права и не входят в группы пользователей, указанные в таблице Субъекты и их права.

   h. Установите флажок Доверенные программы обновления, если вы хотите, чтобы программы, удовлетворяющие условиям срабатывания правила, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready считал доверенными программами обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

6. При миграции параметров Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready осуществляется также миграция списка исполняемых файлов, созданных доверенными программами обновления.

7. Сохраните внесенные изменения.

Добавление условия срабатывания в правило Контроля программ

Чтобы добавить новое условие срабатывания в правило Контроля программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Контроль программ.

   В правой части окна отобразятся параметры компонента Контроль программ.

3. Установите флажок Контроль программ, чтобы параметры компонента стали доступными для изменения.

4. Выполните одно из следующих действий:

   - Если вы хотите создать новое правило и добавить в него условие срабатывания, нажмите на кнопку Добавить.

   - Если вы хотите добавить условие срабатывания в существующее правило, выберите его в списке правил и нажмите на кнопку Изменить.

   Откроется окно Правило Контроля программ.

5. В таблице Включающие условия или Исключающие условия нажмите на кнопку Добавить.

   С помощью раскрывающегося списка под кнопкой Добавить вы можете добавлять в правило различные условия срабатывания (см. инструкции ниже).

Чтобы добавить условие срабатывания правила на основе свойств файлов в указанной папке, выполните следующие действия:

1. В раскрывающемся списке под кнопкой Добавить выберите пункт Условия из свойств файлов указанной папки.

   Откроется стандартное окно Microsoft Windows Выбор папки.

2. В окне Выбор папки выберите папку с исполняемыми файлами программ, на основе свойств которых вы хотите сформировать одно или несколько условий срабатывания правила.

3. Нажмите на кнопку OK.

   Откроется окно Добавление условий.

4. В раскрывающемся списке Показать критерий выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: Хеш файла, Сертификат, KL-категория, Метаданные или Путь к папке.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабатывания правила используется SHA256-хеш.

5. Если в раскрывающемся списке Показать критерий вы выбрали элемент Метаданные, установите флажки напротив тех свойств исполняемых файлов программы, которые вы хотите использовать в условии срабатывании правила: Название файла, Версия файла, Название программы, Версия программы, Производитель.

   Если не выбрано ни одно из указанных свойств, правило не может быть сохранено.

6. Если в раскрывающемся списке Показать критерий вы выбрали элемент Сертификат, установите флажки напротив тех параметров, которые вы хотите использовать в условии срабатывании правила: Издатель, Субъект, Отпечаток.

   Если не выбран ни один из указанных параметров, правило не может быть сохранено.

Не рекомендуется использовать в качестве условий срабатывания правил только критерии Издатель и Субъект. Использование этих критериев является ненадежным.

7. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условия срабатывания правила.

8. Нажмите на кнопку Далее.

   Отобразится список сформированных условий срабатывания правила.

9. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило Контроля программ.

10. Нажмите на кнопку Завершить.

Чтобы добавить условие срабатывания правила на основе свойств программ, запускавшихся на компьютере, выполните следующие действия:

1. В раскрывающемся списке под кнопкой Добавить выберите пункт Условия из свойств запускавшихся программ.

2. В окне Добавление условий в раскрывающемся списке Показать критерий выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: Хеш файла, Сертификат, KL-категория, Метаданные или Путь к папке.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабатывания правила используется SHA256-хеш.

3. Если в раскрывающемся списке Показать критерий вы выбрали элемент Метаданные, установите флажки напротив тех свойств исполняемых файлов программы, которые вы хотите использовать в условии срабатывании правила: Название файла, Версия файла, Название программы, Версия программы, Производитель.

   Если не выбрано ни одно из указанных свойств, правило не может быть сохранено.

4. Если в раскрывающемся списке Показать критерий вы выбрали элемент Сертификат, установите флажки напротив тех параметров, которые вы хотите использовать в условии срабатывании правила: Издатель, Субъект, Отпечаток.

   Если не выбран ни один из указанных параметров, правило не может быть сохранено.

   Не рекомендуется использовать в качестве условий срабатывания правил только критерии Издатель и Субъект. Использование этих критериев является ненадежным.

5. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условия срабатывания правила.

6. Нажмите на кнопку Далее.

   Отобразится список сформированных условий срабатывания правила.

7. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило Контроля программ.

8. Нажмите на кнопку Завершить.

Чтобы добавить условие срабатывания правила на основе KL-категории, выполните следующие действия:

1. В раскрывающемся списке под кнопкой Добавить выберите пункт Условия "KL-категория".

   KL-категория - сформированный специалистами "Лаборатории Касперского" список программ, обладающих общими тематическими признаками. Например, KL-категория "Офисные программы" включает в себя программы из пакетов Microsoft O ice, Adobe® Acrobat® и другие.

2. В окне Условия "KL-категория" установите флажки около названий тех KL-категорий, на основе которых вы хотите создать условия срабатывания правила.

3. Нажмите на кнопку OK.

Чтобы добавить условие срабатывания правила, сформированное вручную, выполните следующие действия:

1. В раскрывающемся списке под кнопкой Добавить выберите пункт Условие вручную.

2. Нажмите на кнопку Выбрать в окне Пользовательское условие и укажите путь к исполняемому файлу программы.

3. Выберите критерий, на основе которого вы хотите создать условие срабатывания правила: Хеш файла, Сертификат, Метаданные или Путь к файлу или папке.

   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабатывания правила используется SHA256-хеш.

   Если вы используете символьную ссылку в поле Путь к файлу или папке, рекомендуется развернуть символьную ссылку для корректной работы правила Контроля программ. Для этого нажмите на кнопку Развернуть символьную ссылку.

4. Настройте параметры выбранного критерия.

5. Нажмите на кнопку OK.

Чтобы добавить условие срабатывания на основе информации о носителе исполняемого файла программы, выполните следующие действия:

1. В раскрывающемся списке под кнопкой Добавить выберите пункт Условие по носителю файла.

2. В окне Условие по носителю файла в раскрывающемся списке Носитель выберите тип запоминающего устройства, запуск программ с которого будет условием срабатывания правила.

3. Нажмите на кнопку OK.

Изменение статуса правила Контроля программ

Чтобы изменить статус правила Контроля программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Контроль программ.

3. Установите флажок Контроль программ, чтобы параметры компонента стали доступными для изменения.

4. В графе Статус по левой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:

   - Вкл. Статус означает, что правило используется во время работы компонента Контроль программ.
   - Выкл. Статус означает, что правило не используется во время работы компонента Контроль программ.
   - Тест. Статус означает, что Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready всегда разрешает запуск программ, на которые распространяется действие этого правила, но заносит информацию о запуске этих программ в отчет.

     С помощью статуса Тест вы можете назначить действие, аналогичное элементу Тестировать правила, для части правил, при выбранном элементе Применять правила в раскрывающемся списке Действие.

5. Сохраните внесенные изменения.

Тестирование правил Контроля программ

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля программ и проанализировать их работу.

Для анализа работы правил Контроля программ требуется изучить события по результатам работы компонента Контроль программ, приходящие в Kaspersky Security Center. Если для всех программ, которые необходимы для работы пользователю компьютера, отсутствуют события о запрете запуска в тестовом режиме, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами правил, создать дополнительные или удалить существующие правила.

По умолчанию для правил Контроля программ выбрано действие Применять правила.

Чтобы включить тестирование правил Контроля программ или выбрать блокирующее действие Контроля программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль программ.
3. Установите флажок Контроль программ, чтобы параметры компонента стали доступными для изменения.
4. В раскрывающемся списке Режим контроля выберите один из следующих элементов:
   - Черный список, если вы хотите разрешать запуск всех программ, кроме программ, указанных в запрещающих правилах.
   - Белый список, если вы хотите запрещать запуск всех программ, кроме программ, указанных в разрешающих правилах.
5. Выполните одно из следующих действий:
   - Если вы хотите включить тестовый режим для правил Контроля программ, в раскрывающемся списке Действие выберите элемент Тестировать правила.
   - Если вы хотите включить блокирующий режим для правил Контроля программ, в раскрывающемся списке Действие выберите элемент Применять правила.
6. Сохраните внесенные изменения.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не будет блокировать программы, запуск которых запрещен компонентом Контроль программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

Правила формирования масок имен файлов или папок

Маска имени файла или папки – это представление имени папки или имени и расширения файла с использованием общих символов.

Для формирования маски имени файла или папки вы можете использовать следующие общие символы:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске C, но не в подпапках.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Изменение шаблонов сообщений Контроля программ

Когда пользователь пытается запустить программу, запрещенную правилом Контроля программ, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready выводит сообщение о блокировке запуска программы. Если блокировка запуска программы, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации.

Для сообщения о блокировке запуска программы и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

Чтобы изменить шаблон сообщения, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль программ.
3. Установите флажок Контроль программ, чтобы параметры компонента стали доступными для изменения.
4. Нажмите на кнопку Шаблоны.

   Откроется окно Шаблоны сообщений.
5. Выполните одно из следующих действий:
   - Если вы хотите изменить шаблон сообщения о блокировке запуска программы, выберите закладку Блокировка.
   - Если вы хотите изменить шаблон сообщения для администратора локальной сети организации, выберите закладку Сообщение администратору.
6. Измените шаблон сообщения о блокировке или сообщения администратору. Для этого используйте кнопки По умолчанию и Переменная.
7. Сохраните внесенные изменения.

Контроль устройств

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Контроль устройств управляет доступом пользователей к установленным или подключенным к компьютеру устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных.

Уровни доступа к устройствам

Контроль устройств управляет доступом на следующих уровнях:

- Тип устройства. Например, принтеры, съемные диски, CD/DVD-приводы.

  Вы можете настроить доступ устройств следующим образом:

  - Разрешать – ✓.
  - Запрещать – ⊘.
  - Зависит от шины подключения (кроме Wi-Fi) – .
  - Запрещать с исключениями (только Wi-Fi и портативные устройства (MTP)) – .

- Шина подключения. Шина подключения – интерфейс, с помощью которого устройства подключаются к компьютеру (например, USB, FireWire). Таким образом, вы можете ограничить подключение всех устройств, например, через USB.

  Вы можете настроить доступ устройств следующим образом:

  - Разрешать – ✓.
  - Запрещать – ⊘.

- Доверенные устройства. Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

  Вы можете добавить доверенные устройства по следующим данным:

  - Устройства по идентификатору. Каждое устройство имеет уникальный идентификатор (англ. Hardware ID – HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы. Пример идентификатора устройства:

    `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств.

  - Устройства по модели. Каждое устройство имеет идентификатор производителя (англ. Vendor ID – VID) и идентификатор продукта(англ. Product ID – PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы. Шаблон для ввода VID и PID: `VID_1234&PID_5678`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.

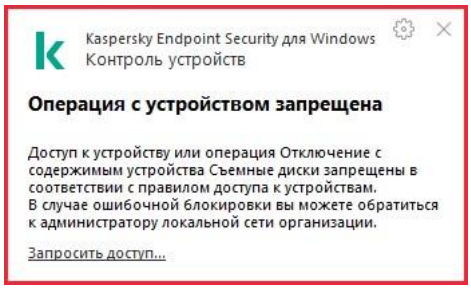
  - Устройства по маске идентификатора. Если вы используете несколько устройств с похожими идентификаторами, вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не поддерживает символ ? при вводе маски. Например, `WDC_C*`.

- Устройства по маске модели. Если вы используете несколько устройств с похожими VID или PID (например, устройства одного производителя), вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не поддерживает символ `?` при вводе маски. Например, `VID_05AC&PID_*`.

Контроль устройств регулирует доступ пользователей к устройствам с помощью правил доступа. Также Контроль устройств позволяет сохранять события подключения / отключения устройств. Для сохранения событий вам нужно настроить отправку событий в политике.

Если доступ к устройству зависит от шины подключения (статус), Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не сохраняет события подключения / отключения устройства. Чтобы программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready сохраняла события подключения / отключения устройства, разрешите доступ к соответствующему типу устройств (статус) или добавьте устройство в список доверенных.

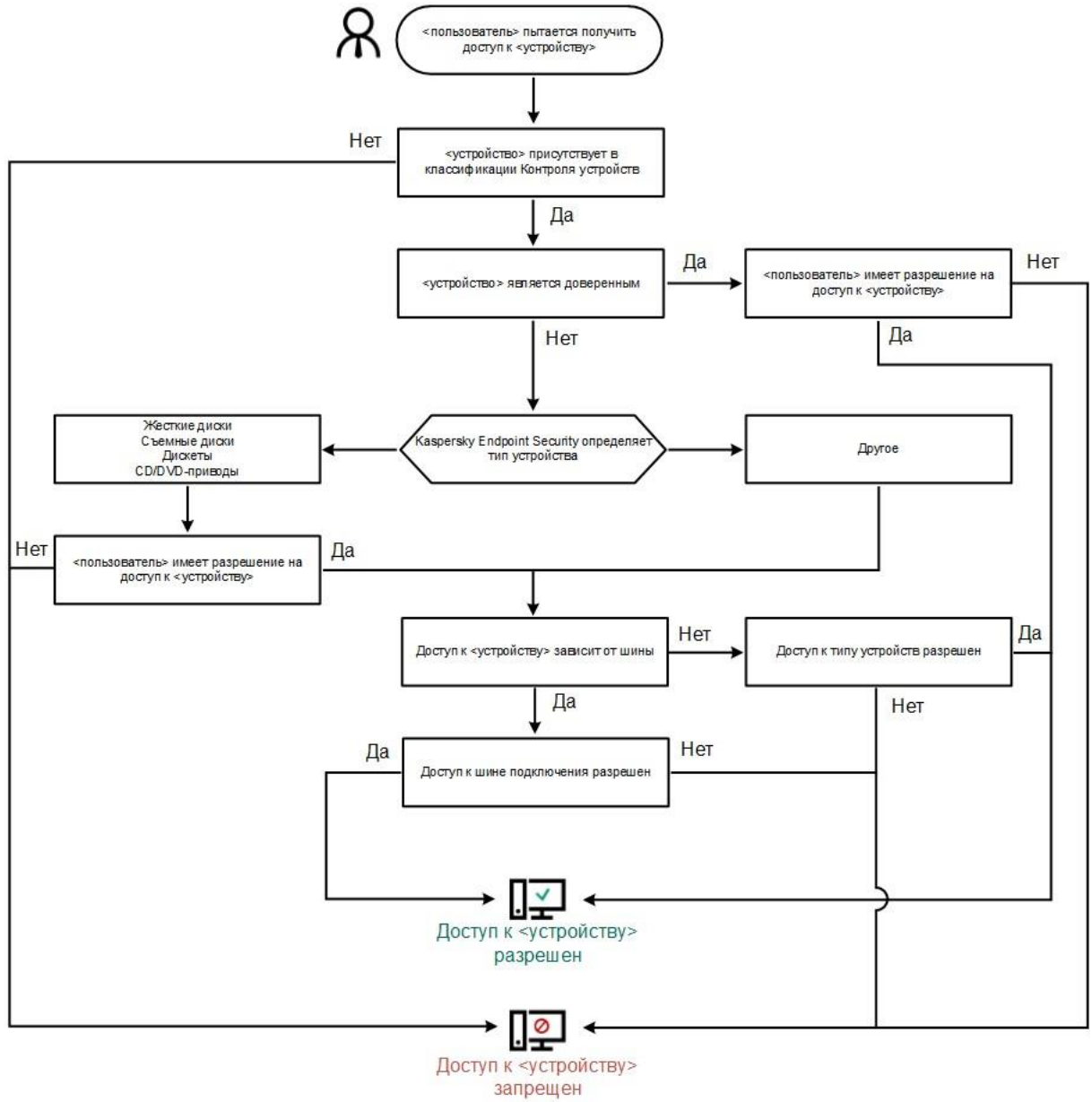
При подключении к компьютеру устройства, доступ к которому запрещен Контролем устройств, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready заблокирует доступ и покажет уведомление (см. рис. ниже).



Уведомление Контроля устройств

Алгоритм работы Контроля устройств

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready принимает решение о доступе к устройству после того, как пользователь подключил это устройство к компьютеру (см. рис. ниже).



Алгоритм работы Контроля устройств

Если устройство подключено и доступ разрешен, вы можете изменить правило доступа и запретить доступ. В этом случае при очередном обращении к устройству (просмотр дерева папок, чтение, запись) Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready блокирует доступ. Блокирование устройства без файловой системы произойдет только при последующем подключении устройства.

Если пользователю компьютера с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready требуется запросить доступ к устройству, которое, по его мнению, было заблокировано ошибочно, передайте ему инструкцию по запросу доступа.

Включение и выключение Контроля устройств

По умолчанию Контроль устройств включен.

Чтобы включить или выключить Контроль устройств, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. Выполните одно из следующих действий:
   - Установите флажок Контроль устройств, если вы хотите включить Контроль устройств.
   - Снимите флажок Контроль устройств, если вы хотите выключить Контроль устройств.
4. Сохраните внесенные изменения.

О правилах доступа

Правила доступа – набор параметров, которые определяют доступ пользователей к установленным или подключенным к компьютеру устройствам. Невозможно добавить устройство, которое выходит за рамки классификации Контроля устройств. Доступ к этим устройствам разрешен для всех пользователей.

Правила доступа к устройствам

Набор параметров правила доступа отличается в зависимости от типа устройств (см. таблицу ниже).

Параметры правила доступа

Устройства	Доступ (✓ /⊘)	Расписание доступа к устройству	Назначение пользователей / группы пользователей	Разрешение на чтение / запись
Жесткие диски	✓	✓	✓	✓
Съемные диски	✓	✓	✓	✓
Принтеры	✓	–	–	–
Дискеты	✓	✓	✓	✓
CD/DVD-приводы	✓	✓	✓	✓
Модемы	✓	–	–	–
Стримеры	✓	–	–	–
Мультифункциональные устройства	✓	–	–	–
Устройства чтения смарт-карт	✓	–	–	–

Windows CE USB ActiveSync устройства	✓	–	–	–
Внешние сетевые адаптеры	✓	–	–	–
Портативные устройства (MTP)	✓	✓	✓	✓
Bluetooth	✓	–	–	–
Камеры и сканеры	✓	–	–	–

Мобильные устройства под управлением Android и iOS относятся к портативным устройствам (MTP). При подключении мобильного устройства к компьютеру операционная система определяет тип устройства. Если на компьютере установлены программы Android Debug Bridge (ADB), iTunes или их аналоги, операционная система определяет мобильные устройства как ADB- или iTunes-устройства. В остальных случаях операционная система может определить тип мобильного устройства как портативное устройство (MTP) для передачи файлов, PTP-устройство (камера) для передачи изображений или другое устройство. Тип устройства зависит от модели мобильного устройства.

Доступ к ADB- или iTunes-устройствам имеет следующие особенности:

- Настроить расписание доступа к устройству невозможно. То есть, если доступ к устройствам ограничен правилами (статус), ADB- и iTunes-устройства доступны всегда.
- Настроить доступ к устройству для отдельных пользователей, а также настроить права доступа (чтение / запись) невозможно. То есть, если доступ к устройствам ограничен правилами (статус), ADB- и iTunesустройства доступны всем пользователям со всеми правами.
- Настроить доступ к доверенным ADB- или iTunes-устройствам для отдельных пользователей невозможно. Если устройство доверенное, ADB- и iTunes-устройства доступны всем пользователям.
- Если вы установили программы ADB или iTunes после подключения устройства к компьютеру, уникальный идентификатор устройства может быть сброшен. То есть, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready определит это устройство как новое. Если устройство доверенное, добавьте устройство в список доверенных повторно.

По умолчанию правила доступа к устройствам разрешают полный доступ к устройствам всем пользователям в любое время, если разрешен доступ к шинам подключения для соответствующих типов устройств (статус).

Правило доступа к сетям Wi-Fi

Правило доступа к сетям Wi-Fi определяет разрешение (статус ✓) или запрет (статус ⊘) на использование сетей Wi-Fi. Вы можете добавить в правило доверенную сеть Wi-Fi (статус). Использование

доверенной сети Wi-Fi разрешено без ограничений. По умолчанию правило доступа к сетям Wi-Fi разрешает доступ к любым сетям Wi-Fi.

Правила доступа к шинам подключения

Правила доступа к шинам определяют только разрешение (статус ✓) или запрет (статус ⊘) на подключение устройств. Для всех шин подключения из классификации компонента Контроль устройств по умолчанию созданы правила, разрешающие доступ к шинам.

Изменение правила доступа к устройствам

В зависимости от типа устройства вы можете изменять разные параметры доступа: список пользователей, получающих доступ к устройству, расписание доступа и разрешение / запрет на доступ.

Чтобы изменить правило доступа к устройствам, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. В правой части окна выберите закладку Типы устройств.

   На закладке Типы устройств находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
4. Выберите правило доступа, которое хотите изменить.
5. Нажмите на кнопку Изменить. Кнопка доступна только для тех типов устройств, которые имеют файловую систему.

   Откроется окно Настройка правила доступа к устройствам.

   По умолчанию правило доступа к устройствам разрешает полный доступ к типу устройств всем пользователям в любое время. Такое правило доступа в списке Пользователи и / или группы пользователей содержит группу Все, а в таблице Права выделенной группы пользователей по расписаниям доступа содержит расписание доступа к устройствам Расписание по умолчанию с установленными правами на все возможные операции с устройствами.
6. Нажмите на кнопку Выбрать.

   Откроется окно Выбор пользователей и/или групп.
7. Выполните следующие действия:

   - Если вы хотите добавить пользователей и / или группы пользователей в таблицу в окне Выбор пользователей и/или групп, выполните следующие действия:

     a. В окне Выбор пользователей и/или групп нажмите на на кнопку Добавить

        Откроется стандартное окно Microsoft Windows Выбор пользователей или групп.

     b. В окне Windows Выбор пользователей или групп задайте пользователей и / или группы пользователей, для которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready распознает выбранные устройства как доверенные.

c. В окне Windows Выбор пользователей или групп нажмите на кнопку OK.

Имена пользователей и / или групп пользователей, заданных в окне Microsoft Windows Выбор пользователей или групп, отобразятся в окне Выбор пользователей и/или групп.

- Если вы хотите удалить пользователей и / или группы пользователей из таблицы в окне Выбор пользователей и/или групп, выберите одну или несколько строк в таблице и нажмите на кнопку Удалить.

  Чтобы выбрать несколько строк, выделяйте их, удерживая клавишу CTRL.

8. В окне Выбор пользователей и/или групп нажмите на кнопку OK.

9. В таблице Права выделенной группы пользователей по расписаниям доступа настройте расписание доступа к устройствам для выбранного пользователя и / или группы пользователей. Для этого установите флажки около названий тех расписаний доступа к устройствам, которые вы хотите использовать в изменяемом правиле доступа к устройствам.

10. Для изменения списка расписаний доступа к устройствам используйте кнопки Создать, Изменить, Копировать, Удалить в таблице Права выделенной группы пользователей по расписаниям доступа.

11. Для каждого расписания доступа к устройствам, используемого в изменяемом правиле, задайте операции, которые разрешаются при работе с устройствами. Для этого в таблице Права выделенной группы пользователей по расписаниям доступа установите флажки в графах с названиями нужных операций.

12. Нажмите на кнопку OK.

    После того как вы изменили исходные значения параметров правила доступа к устройствам, параметр доступа к типу устройств в графе Доступ в таблице на закладке Типы устройств принимает значение Ограничивать правилами.

13. Сохраните внесенные изменения.

Включение и выключение записи событий в журнал

Запись событий в журнал доступна только для операций с файлами на съемных дисках.

Чтобы включить или выключить запись событий в журнал, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.

3. В правой части окна выберите закладку Типы устройств.

   На закладке Типы устройств находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. Выберите в таблице устройств Съемные диски.

   В верхней части таблицы станет доступной кнопка Запись событий в журнал.

5. Нажмите на кнопку Запись событий в журнал.

Откроется окно Параметры записи событий в журнал.

6. Выполните одно из следующих действий:

   - Если вы хотите включить запись событий об операциях записи и удаления файлов на съемных дисках, установить флажок Включить запись событий в журнал.

     Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready будет сохранять событие в файл журнала и отправлять сообщение на Сервер администрирования Kaspersky Security Center, когда пользователь совершает операции записи или удаления с файлами на съемных дисках.

   - В противном случае снимите флажок Включить запись событий в журнал.

7. Укажите, информация о каких операциях должна записываться в журнал. Для этого выполните одно из следующих действий:

   - Если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready записывал в журнал все события, установите флажок Все форматы.

   - Если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready записывал в журнал только информацию о файлах определенного формата, в блоке Фильтр по форматам файлов установите флажки напротив нужных форматов файлов.

8. Нажмите на кнопку Выбрать.

   Откроется окно Выбор пользователей и/или групп.

   Когда пользователи, указанные в блоке Пользователи, будут производить запись в файлы, расположенные на съемных дисках, или удалять файлы со съемных дисков, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready будет сохранять информацию о совершенной операции в журнал событий и отправлять сообщение на Сервер администрирования Kaspersky Security Center.

9. Выполните следующие действия:

   - Если вы хотите добавить пользователей и / или группы пользователей в таблицу в окне Выбор пользователей и/или групп, выполните следующие действия:

     1. В окне Выбор пользователей и/или групп нажмите на на кнопку Добавить

        Откроется стандартное окно Microsoft Windows Выбор пользователей или групп.

     2. В окне Windows Выбор пользователей или групп задайте пользователей и / или группы пользователей, для которых Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready распознает выбранные устройства как доверенные.

     3. В окне Windows Выбор пользователей или групп нажмите на кнопку OK.

        Имена пользователей и / или групп пользователей, заданных в окне Microsoft Windows Выбор пользователей или групп, отобразятся в окне Выбор пользователей и/или групп.

   - Если вы хотите удалить пользователей и / или группы пользователей из таблицы в окне Выбор пользователей и/или групп, выберите одну или несколько строк в таблице и нажмите на кнопку Удалить.

     Чтобы выбрать несколько строк, выделяйте их, удерживая клавишу CTRL.

10. Сохраните внесенные изменения.

Вы можете просмотреть события, связанные с файлами на съемных дисках, в Консоли администрирования Kaspersky Security Center в рабочей области для узла Сервер администрирования на закладке События. Чтобы события отображались в локальном журнале событий Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, требуется установить флажок Выполнена операция с файлом в параметрах уведомлений для компонента Контроль устройств.

Добавление сети Wi-Fi в список доверенных

Вы можете разрешить пользователям подключаться к сетям Wi-Fi, которые вы считаете безопасными, например, к корпоративной сети Wi-Fi. Для этого нужно добавить эту сеть в список доверенных сетей Wi-Fi. Контроль устройств будет блокировать доступ ко всем сетям Wi-Fi, кроме тех, которые указаны в списке доверенных.

Чтобы добавить сеть Wi-Fi в список доверенных, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. В правой части окна выберите закладку Типы устройств.

   На закладке Типы устройств находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
4. В графе Доступ напротив устройства Wi-Fi вызовите контекстное меню по правой клавише мыши.
5. Выберите пункт Запрещать с исключениями.
6. В списке устройств выберите Wi-Fi и нажмите на кнопку Изменить.

   Откроется окно Доверенные сети Wi-Fi.
7. Нажмите на кнопку Добавить.

   Откроется окно Доверенная сеть Wi-Fi.
8. В окне Доверенная сеть Wi-Fi выполните следующие действия:

   - В поле Имя сети укажите имя сети Wi-Fi, которую вы хотите добавить в список доверенных.
   - В раскрывающемся списке Тип аутентификации выберите тип аутентификации, используемый при подключении к доверенной сети Wi-Fi.
   - В раскрывающемся списке Тип шифрования выберите тип шифрования, используемый для защиты трафика доверенной сети Wi-Fi.
   - В поле Комментарий вы можете указать любую информацию о добавленной сети Wi-Fi.

   Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.
9. Сохраните внесенные изменения.

Изменение правила доступа к шине подключения

Чтобы изменить правило доступа к шине подключения, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. Выберите закладку Шины подключения.

   На закладке Шины подключения находятся правила доступа для всех шин подключения, которые есть в классификации компонента Контроль устройств.
4. Выберите правило доступа к шине, которое хотите изменить.
5. Измените значение параметра доступа:

   - Чтобы разрешить доступ к шине подключения, в графе Доступ вызовите контекстное меню и выберите пункт Разрешать.
   - Чтобы запретить доступ к шине подключения, в графе Доступ вызовите контекстное меню и выберите пункт Запрещать.
6. Сохраните внесенные изменения.

Действия с доверенными устройствами

.Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Для работы с доверенными устройствами вы можете предоставить доступ отдельному пользователю, группе пользователей или всем пользователям организации.

Например, если в вашей организации запрещено использование съемных дисков, но администраторы используют съемные диски в своей работе, вы можете разрешить использование съемных дисков только для группы администраторов. Для этого необходимо добавить съемные диски в список доверенных и настроить права доступа пользователей.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет добавить устройство в список доверенных следующими способами:

- Если в вашей организации не развернуто решение Kaspersky Security Center, вы можете подключить устройство к компьютеру и добавить его в список доверенных в параметрах программы. Чтобы распространить список доверенных устройств на все компьютеры организации, вы можете включить функцию объединения списков доверенных устройств в политике или использовать процедуру экспорта / импорта.
- Если в вашей организации развернуто решение Kaspersky Security Center, вы можете обнаружить все подключенные устройства удаленно и создать список доверенных устройств в политике. Список доверенных устройств будет доступен на всех компьютерах, к которым применена политика.

Добавление устройства в список доверенных из интерфейса программы

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей "Все").

Чтобы добавить устройство в список доверенных из интерфейса программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. В правой части окна выберите закладку Доверенные устройства.
4. Нажмите на кнопку Выбрать.

   Откроется окно Выбор доверенных устройств.
5. Установите флажок напротив названия устройства, которое вы хотите добавить в список доверенных устройств.

   Список устройств в графе Устройства зависит от того, какое значение выбрано в раскрывающемся списке Отображать подключенные устройства.
6. Нажмите на кнопку Выбрать.

   Откроется окно Выбор пользователей и/или групп.
7. Выполните следующие действия:

   - Если вы хотите добавить пользователей и / или группы пользователей в таблицу в окне Выбор пользователей и/или групп, выполните следующие действия:

     a. В окне Выбор пользователей и/или групп нажмите на на кнопку Добавить

        Откроется стандартное окно Microsoft Windows Выбор пользователей или групп.

     b. В окне Windows Выбор пользователей или групп задайте пользователей и / или группы пользователей, для которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready распознает выбранные устройства как доверенные.

     c. В окне Windows Выбор пользователей или групп нажмите на кнопку OK.

        Имена пользователей и / или групп пользователей, заданных в окне Microsoft Windows Выбор пользователей или групп, отобразятся в окне Выбор пользователей и/или групп.

   - Если вы хотите удалить пользователей и / или группы пользователей из таблицы в окне Выбор пользователей и/или групп, выберите одну или несколько строк в таблице и нажмите на кнопку Удалить.

     Чтобы выбрать несколько строк, выделяйте их, удерживая клавишу CTRL.
8. В окне Выбор пользователей и/или групп нажмите на кнопку OK.
9. Нажмите на кнопку OK.
10. В окне Выбор доверенных устройств нажмите на кнопку OK.

В таблице на закладке Доверенные устройства окна настроек компонента Контроль устройств появится строка с параметрами добавленного доверенного устройства.

11. Повторите пункты 4-7 для каждого устройства, которое вы хотите добавить в список доверенных устройств для определенных пользователей и / или групп пользователей.

12. Сохраните внесенные изменения.

Добавление устройства в список доверенных из Kaspersky Security Center

Kaspersky Security Center получает информацию об устройствах, если на компьютерах установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и включен Контроль устройств. Добавить устройство в список доверенных, информации о котором в Kaspersky Security Center нет, невозможно.

Вы можете добавить устройство в список доверенных по следующим данным:

- Устройства по идентификатору. Каждое устройство имеет уникальный идентификатор (англ. Hardware ID – HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы. Пример идентификатора устройства: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств.

- Устройства по модели. Каждое устройство имеет идентификатор производителя (англ. Vendor ID – VID) и идентификатор продукта(англ. Product ID – PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы. Шаблон для ввода VID и PID: `VID_1234&PID_5678`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.

- Устройства по маске идентификатора. Если вы используете несколько устройств с похожими идентификаторами, вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не поддерживает символ ? при вводе маски. Например, `WDC_C*`.

- Устройства по маске модели. Если вы используете несколько устройств с похожими VID или PID (например, устройства одного производителя), вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не поддерживает символ `?` при вводе маски. Например, `VID_05AC&PID_*`.

Чтобы добавить устройства в список доверенных, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку Политики.

4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

5. В окне политики выберите Контроль безопасности → Контроль устройств.

6. В правой части окна выберите закладку Доверенные устройства.

7. Установите флажок Объединять значения при наследовании, если вы хотите создать общий список доверенных устройств для всех компьютеров организации.

   Списки доверенных устройств родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные устройства родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных устройств родительской политики невозможно.

8. Нажмите на кнопку Добавить и выберите способ добавления устройства в список доверенных.

9. Для фильтрации устройств в раскрывающемся списке Тип устройств выберите тип устройств (например, Съемные диски).

10. В поле Название / Модель введите идентификатор устройства, модель (VID и PID) или маску в зависимости от выбранного способа добавления.

    Способ добавления устройств по маске модели (VID и PID) имеет особенность. Если вы ввели маску модели, которая не соответствует ни одной модели, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready проверяет идентификатор устройства (HWID) на соответствие маске. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready проверяет на соответствие только часть идентификатора устройства, определяющую поставщика и тип устройства (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Если маска модели соответствует этой части идентификатора устройства, на компьютере в список доверенных устройств будут добавлены устройства удовлетворяющие маске. При этом в Kaspersky Security Center по кнопке Обновить отобразится пустой список устройств. Для корректного отображения списка устройств вы можете использовать способ добавления по маске идентификатора устройства.

11. Для фильтрации устройств в поле Компьютер введите имя компьютера или маску имени компьютера, к которому подключено устройство.

    Символ `*` заменяет любой набор символов. Символ `?` заменяет любой один символ.

12. Нажмите на кнопку Обновить.

    В таблице отобразится список устройств, которые удовлетворяют заданным параметрам фильтрации.

13. Установите флажки напротив названий устройств, которые вы хотите добавить в список доверенных.

14. В поле Комментарий введите описание причины добавления устройств в список доверенных.

15. Справа от поля Разрешать пользователям и / или группам пользователей нажмите на кнопку Выбрать.

16. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.

    По умолчанию доступ к доверенным устройствам разрешен для группы "Все".

17. Сохраните внесенные изменения.

При подключении устройства Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready проверяет список доверенных устройств для авторизованного пользователя. Если устройство доверенное, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready разрешает доступ к

устройству со всеми правами, даже если доступ к типу устройств или шине подключения запрещен. Если устройство недоверенное и доступ запрещен, вы можете запросить доступ к заблокированному устройству.

Экспорт и импорт списка доверенных устройств

Для распространения список доверенных устройств на всех компьютеры организации вы можете использовать процедуру экспорта / импорта.

Например, если вам нужно распространить список доверенных съемных дисков, нужно выполнить следующие действия:

1. Последовательно подключите съемные диски к компьютеру.
2. В параметрах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавьте съемные диски в список доверенных. Если требуется, настройте права доступа пользователей. Например, разрешите доступ к съемным дискам только администраторам.
3. Экспортируйте список доверенных устройств в параметрах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (см. инструкцию ниже).
4. Распространите файл с списком доверенных устройств на остальные компьютеры организации. Например, разместите файл в общей папке.
5. Импортируйте список доверенных устройств в параметрах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на остальных компьютерах организации (см. инструкцию ниже).

Чтобы импортировать или экспортировать список доверенных устройств, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. В правой части окна выберите закладку Доверенные устройства.
4. Для экспорта списка доверенных устройств, выполните следующие действия:
   a. Нажмите на кнопку Экспорт.
   b. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список доверенных устройств, а также выберите папку, в которой вы хотите сохранить этот файл.

      Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready экспортирует весь список доверенных устройств в XML-файл.
5. Для импорта списка доверенных устройств, выполните следующие действия:
   a. Нажмите на кнопку Импорт.
   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных устройств.

Если на компьютере уже есть список доверенных устройств, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предложит удалить действующий список или добавить в него новые записи из XML-файла.

6. Сохраните внесенные изменения.

При подключении устройства Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет список доверенных устройств для авторизованного пользователя. Если устройство доверенное, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает доступ к устройству со всеми правами, даже если доступ к типу устройств или шине подключения запрещен.

Получение доступа к заблокированному устройству

При настройке Контроля устройств вы можете случайно запретить доступ к необходимому для работы устройству.

Если в вашей организации не развернуто решение Kaspersky Security Center, то вы можете предоставить доступ к устройству в параметрах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Например, вы можете добавить устройство в список доверенных или временно выключить Контроль устройств.

Если в вашей организации развернуто решение Kaspersky Security Center и к компьютерам применена политика, вы можете предоставить доступ к устройству в Консоли администрирования.

Онлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в онлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. Компьютер должен иметь возможность установить связь с Сервером администрирования.

Предоставление доступа в онлайн-режиме состоит из следующих этапов:

1. Пользователь отправляет администратору сообщение с запросом на предоставление доступа.

2. Администратор добавляет устройство в список доверенных.

   Вы можете добавить доверенное устройство в политике для группы администрирования или в локальных параметрах программы для отдельного компьютера.

3. Администратор обновляет параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на компьютере пользователя.

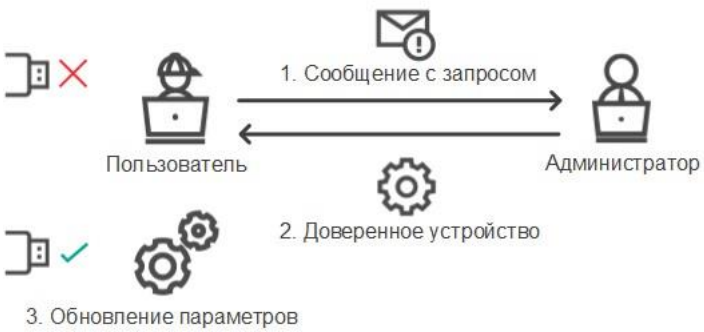


Схема предоставления доступа к устройству в онлайн-режиме

Офлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в офлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. В параметрах политики в разделе Контроль устройств должен быть установлен флажок Разрешить запрашивать временный доступ.

Если вам необходимо предоставить временный доступ к заблокированному устройству, а добавить устройство в список доверенных невозможно, вы можете предоставить доступ к устройству в офлайнрежиме. Таким образом, вы можете предоставить доступ к заблокированному устройству, если у компьютера отсутствует доступ к сети или компьютер находится за пределами сети организации.

Предоставление доступа в офлайн-режиме состоит из следующих этапов:

1. Пользователь создает файл запроса и передает его администратору.
2. Администратор создает из файла запроса ключ доступа и передает его пользователю.
3. Пользователь активирует ключ доступа.

Схема предоставления доступа к устройству в офлайн-режиме

Онлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в онлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. Компьютер должен иметь возможность установить связь с Сервером администрирования.

Чтобы пользователю запросить доступ к заблокированному устройству, выполните следующие действия:

1. Подключите устройство к компьютеру.

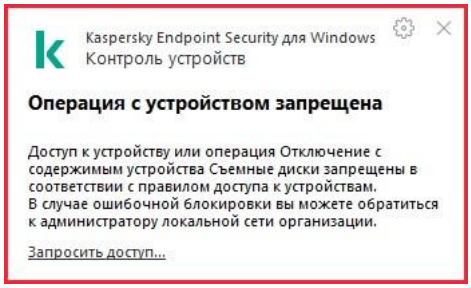
   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready покажет уведомление блокировки доступа к устройству (см. рис. ниже).

2. Нажмите на ссылку Запросить доступ.

   Откроется окно Сообщение для администратора. В сообщении содержится информация о заблокированном устройстве.

3. Нажмите на кнопку Отправить.

Администратор получит сообщение с запросом на предоставление доступа, например, по электронной почте. Подробнее об обработке запросов пользователей см. в справке Kaspersky Security Center. После добавления устройства в список доверенных и обновления параметров Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready на компьютере пользователь получит доступ к устройству.



Уведомление Контроля устройств

Офлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в офлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. В параметрах политики в разделе Контроль устройств должен быть установлен флажок Разрешить запрашивать временный доступ.

Чтобы пользователю запросить доступ к заблокированному устройству, выполните следующие действия:

1. Подключите устройство к компьютеру.

   Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready покажет уведомление блокировки доступа к устройству.

2. Нажмите на ссылку Запросить временный доступ.

   Откроется окно Запрос доступа к устройству со списком подключенных устройств.

3. В списке подключенных устройств выберите устройство, к которому вы хотите получить доступ.

4. Нажмите на кнопку Сформировать файл запроса.

5. В поле Длительность доступа к устройству укажите, на какое время вы хотите получить доступ к устройству.

6. Сохраните файл в память компьютера.

В результате в память компьютера будет загружен файл запроса с расширением *.akey. Передайте файл запроса доступа к устройству администратору локальной сети организации любым доступным способом.

Чтобы администратору создать ключ доступа к заблокированному устройству, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку Устройства.
4. В списке клиентских компьютеров выберите компьютер, пользователю которого вы хотите дать временный доступ к заблокированному устройству.
5. В контекстном меню компьютера выберите пункт Предоставление доступа в офлайн-режиме.
6. В открывшемся окне выберите закладку Контроль устройств.
7. Нажмите на кнопку Обзор и загрузите полученный от пользователя файл запроса.

   Отобразится информация о заблокированном устройстве, к которому пользователь запросил доступ.
8. Если требуется, измените значение параметра Длительность доступа к устройству.

   По умолчанию для параметра Длительность доступа к устройству выбрано значение, указанное пользователем при формировании файла запроса.
9. Укажите значение параметра Срок активации.

   Параметр содержит период времени, в течение которого пользователь может активировать доступ к заблокированному устройству с помощью предоставленного ключа доступа.
10. Сохраните файл ключа доступа в память компьютера.

В результате в память компьютера будет загружен ключ доступа к заблокированному устройству. Файл ключа доступа имеет расширение *.acode. Передайте ключ доступа к заблокированному устройству пользователю любым доступным способом.

Чтобы пользователю активировать ключ доступа, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. В правой части окна нажмите на кнопку Запросить доступ.
4. В окне Запрос доступа к устройству нажмите на кнопку Активировать ключ доступа.
5. В открывшемся окне выберите файл с ключом доступа к устройству, полученный от администратора локальной сети организации. Нажмите на кнопку Открыть.

   Откроется окно с информацией о предоставленном доступе.

6. Нажмите на кнопку OK.

В результате пользователь получит доступ к устройству на срок, установленный администратором. Пользователь получит полный набор прав доступа к устройству (запись и чтение). По истечении срока действия ключа доступ к устройству будет заблокирован. Если пользователю требуется постоянный доступ к устройству, добавьте устройство в список доверенных.

Изменение шаблонов сообщений Контроля устройств

Когда пользователь пытается обратиться к заблокированному устройству, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выводит сообщение о блокировке доступа к устройству или о запрете операции над содержимым устройства. Если блокировка доступа к устройству или запрет операции с содержимым устройства, по мнению пользователя, произошло ошибочно, пользователь может отправить сообщение администратору локальной сети организации по ссылке из текста сообщения о блокировке.

Для сообщения о блокировке доступа к устройству или запрете операции над содержимым устройства, а также для сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

Чтобы изменить шаблоны сообщений Контроля устройств, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. В правой части окна нажмите на кнопку Шаблоны.

   Откроется окно Шаблоны сообщений.
4. Выполните одно из следующих действий:
   - Если вы хотите изменить шаблон сообщения о блокировке доступа к устройству или о запрете операции над содержимым устройства, выберите закладку Блокировка.
   - Если вы хотите изменить шаблон сообщения администратору локальной сети организации, выберите закладку Сообщение администратору.
5. Измените шаблон сообщения. При этом вы можете использовать кнопки Переменная, По умолчанию и Ссылка (кнопка доступна только на закладке Блокировка).
6. Сохраните внесенные изменения.

Лучшие практики по внедрению режима белого списка

При планировании внедрения режима белого списка рекомендуется выполнить следующие действия:

1. Произвести следующие виды группировок:
   - Группы пользователей. Группы пользователей, для которых необходимо разрешить использование различных наборов программ.

- Группы администрирования. Одна или несколько групп компьютеров, к которым Kaspersky Security Center будет применять режим белого списка. Создание нескольких групп компьютеров необходимо, если для этих групп используются различные параметры режима белого списка.

2. Составить список программ, запуск которых необходимо разрешить.

   Перед составлением списка рекомендуется выполнить следующие действия:

   a. Запустить задачу инвентаризации.

      Информация о создании, изменении параметров и запуске задачи инвентаризации доступна в разделе Управление задачами.

   b. Просмотреть список исполняемых файлов.

Настройка режима белого списка

При настройке режима белого списка рекомендуется выполнить следующие действия:

1. Создать категории программ, содержащие те программы, запуск которых необходимо разрешить.

   Вы можете выбрать один из следующих способов формирования категорий программ:

   - Пополняемая вручную категория. Вы можете вручную пополнять эту категорию, используя следующие условия:
     - Метаданные файла. Kaspersky Security Center добавляет в категорию программ все исполняемые файлы, сопровождающиеся указанными метаданными.
     - Хеш файла. Kaspersky Security Center добавляет в категорию программ все исполняемые файлы, имеющие указанный хеш.

       Использование этого условия исключает возможность автоматической установки обновлений, поскольку файлы различных версий будут иметь различный хеш.

     - Сертификат файла. Kaspersky Security Center добавляет в категорию программ все исполняемые файлы, подписанные указанным сертификатом.
     - KL-категория. Kaspersky Security Center добавляет в категорию программ все программы, входящие в указанную KL-категорию.
     - Папка программы. Kaspersky Security Center добавляет в категорию программ все исполняемые файлы из этой папки.

       Использование условия "Папка программы" небезопасно, поскольку запуск любой программы из указанной папки будет разрешен. Правила, использующие категории программ с условием "Папка программы", рекомендуется применять только к тем пользователям, для которых необходимо разрешить автоматическую установку обновлений.

- Категория, в которую входят исполняемые файлы из указанной папки. Вы можете указать папку, исполняемые файлы из которой будут автоматически попадать в создаваемую категорию программ.

- Категория, в которую входят исполняемые файлы с выбранных устройств. Вы можете указать компьютер, все исполняемые файлы которого будут автоматически попадать в создаваемую категорию программ.

  При использовании этого способа формирования категорий программ Kaspersky Security Center получает информацию о программах на компьютере из папки Исполняемые файлы.

2. Выбрать режим белого списка для компонента Контроль программ.

3. Создать правила Контроля программ с использованием созданных категорий программ.

   Для режима белого списка изначально заданы правило Операционная система и ее компоненты, которое разрешает запуск программ, входящих в KL-категорию "Программы ОС", и правило Доверенные программы обновления, которое разрешает запуск программ, входящих в KLкатегорию "Доверенные программы обновления". В KL-категорию "Программы ОС" входят программы, обеспечивающие нормальную работу операционной системы. В KL-категорию "Доверенные программы обновления" входят программы обновления наиболее известных производителей программного обеспечения. Вы не можете удалить эти правила. Параметры этих правил недоступны для изменения. По умолчанию правило Операционная система и ее компоненты включено, а правило Доверенные программы обновления выключено. Запуск программ, соответствующих условиям срабатывания этих правил, разрешен всем пользователям.

4. Определить те программы, для которых необходимо разрешить автоматическую установку обновлений.

   Вы можете разрешить автоматическую установку обновлений одним из следующих способов:

   - Указать расширенный список разрешенных программ, разрешив запуск всех программ, входящих в любую из KL-категорий.

   - Указать расширенный список разрешенных программ, разрешив запуск всех программ, подписанных сертификатами.

     Чтобы разрешить запуск всех программ, подписанных сертификатами, вы можете создать категорию с условием на основе сертификата, в котором используется только параметр Субъект со значением *.

   - Для правила Контроля программ установить параметр Доверенные программы обновления. Если этот флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет считать программы, входящие в правило, доверенными программами обновления. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает запуск программ, которые были установлены или обновлены программами, входящими в правило. При этом программы не должны попадать под действие запрещающих правил.

     При миграции параметров Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready осуществляется также миграция списка исполняемых файлов, созданных доверенными программами обновления.

- Создать папку и поместить в нее исполняемые файлы программ, для которых вы хотите разрешить автоматическую установку обновлений. Далее создать категорию программ с условием "Папка программы" и указать путь к этой папке. Далее создать разрешающее правило и выбрать эту категорию.

  Использование условия "Папка программы" небезопасно, поскольку запуск любой программы из указанной папки будет разрешен. Правила, использующие категории программ с условием "Папка программы", рекомендуется применять только к тем пользователям, для которых необходимо разрешить автоматическую установку обновлений.

Тестирование режима белого списка

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля программ и проанализировать их работу. При включении тестирования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не будет блокировать программы, запуск которых запрещен правилами Контроля программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании режима белого списка рекомендуется выполнить следующие действия:

1. Определить период тестирования (от нескольких дней до двух месяцев).
2. Включить тестирование правил Контроля программ.
3. Проанализировать результаты тестирования, используя события по результатам тестовой работы Компонента программ и отчеты о запрещенных программах в тестовом режиме.
4. По результатам анализа внести изменения в параметры режима белого списка.

   В частности, по результатам тестирования вы можете добавить в категорию программ исполняемые файлы, связанные с событиями.

Поддержка режима белого списка

После выбора блокирующего действия Контроля программ рекомендуется продолжать поддержку режима белого списка, выполняя следующие действия:

- Анализировать работу правил Контроля программ, используя события по результатам работы Контроля программ и отчеты о запрещенных запусках.
- Анализировать запросы доступа к программам, получаемые от пользователей.
- Анализировать незнакомые исполняемые файлы, проверяя их репутацию в Kaspersky Security Network или на портале Kaspersky Whitelist.
- Перед установкой обновлений для операционной системы или для программного обеспечения устанавливать эти обновления на тестовой группе компьютеров, чтобы проверить, как они будут обрабатываться правилами Контроля программ.
- Добавлять необходимые программы в категории, используемые в правилах Контроля программ.

Анти-Бриджинг

Анти-Бриджинг предотвращает создание сетевых мостов, исключая возможность одновременной установки нескольких сетевых соединений для компьютера. Это позволяет защитить корпоративную сеть от атак через незащищенные, несанкционированные сети.

Анти-Бриджинг регулирует установку сетевых соединений с помощью правил установки соединений.

Правила установки соединений созданы для следующих предустановленных типов устройств:

- сетевые адаптеры;
- адаптеры Wi-Fi;
- модемы.

Если правило установки соединений включено, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

- блокирует активное соединение при установке нового соединения, если для обоих соединений используется указанный в правиле тип устройств;
- блокирует соединения, установленные или устанавливаемые с помощью тех типов устройств, для которых используются правила с более низким приоритетом.

Включение и выключение Анти-Бриджинга

По умолчанию функция Анти-Бриджинг выключена.

Чтобы включить или выключить функцию Анти-Бриджинг, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. Нажмите на кнопку Анти-Бриджинг.

   Откроется окно Анти-Бриджинг.
4. Выполните одно из следующих действий:
   - Установите флажок Включить Анти-Бриджинг, чтобы включить защиту от сетевых мостов.

     После включения функции Анти-Бриджинг Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует уже установленные соединения в соответствии с правилами установки соединений.
   - Снимите флажок Включить Анти-Бриджинг, чтобы выключить защиту от сетевых мостов.
5. Сохраните внесенные изменения.

Изменение статуса правила установки соединений

Чтобы изменить статус правила установки соединений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. Нажмите на кнопку Анти-Бриджинг.

   Откроется окно Анти-Бриджинг.
4. Выберите правило, статус которого вы хотите изменить.
5. В графе Контроль откройте контекстное меню по левой клавише мыши и выполните одно из следующих действий:
   - Если вы хотите включить использование правила, выберите пункт Вкл.
   - Если вы хотите выключить использование правила, выберите пункт Выкл.
6. Сохраните внесенные изменения.

Изменение приоритета правила установки соединений

Чтобы изменить приоритет правила установки соединений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Контроль устройств.
3. Нажмите на кнопку Анти-Бриджинг.

   Откроется окно Анти-Бриджинг.
4. Выберите правило, приоритет которого вы хотите изменить.
5. Выполните одно из следующих действий:
   - Нажмите на кнопку Вверх, чтобы переместить правило на уровень выше в таблице правил.
   - Нажмите на кнопку Вниз, чтобы переместить правило на уровень ниже в таблице правил.

   Чем выше правило в таблице правил, тем выше у него приоритет. Функция Анти-Бриджинг блокирует все соединения, кроме одного соединения, установленного с помощью того типа устройств, для которого используется правило с наиболее высоким приоритетом.
6. Сохраните внесенные изменения.

Веб-Контроль

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть вебсайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует доступ или покажет предупреждение (см. рис. ниже).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует только HTTP- и HTTPS-трафик.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

Способы управления доступом к веб-сайтам

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- Категория веб-сайта. Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз программы). Вы можете ограничить доступ пользователей, например, к категории "Социальные сети" или другим категориям.

- Тип данных. Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready определяет тип данных по формату файла, а не по расширению.

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready определит тип данных "Архивы", а не "Графические файлы".

- Отдельный адрес. Вы можете ввести веб-адрес или использовать маски.

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к типу данных "Файлы офисных программ" только для категории веб-сайтов "Веб-почта".

Правила доступа к веб-сайтам

Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью правил доступа. Вы можете настроить следующие дополнительные параметры правила доступа к веб-сайтам:

- Пользователи, на которых распространяется правило.

Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

- Расписание работы правила.

  Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Приоритеты правил доступа

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом. Например, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории веб-сайтов "Социальные сети" и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.

Сообщения Веб-Контроля

Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен.

Чтобы включить или выключить Веб-Контроль, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Веб-Контроль.

3. Выполните одно из следующих действий:

   - Установите флажок Веб-Контроль, если вы хотите включить Веб-Контроль.
   - Снимите флажок Веб-Контроль, если вы хотите выключить Веб-Контроль.

   Если Веб-Контроль выключен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не контролирует доступ к веб-ресурсам.

4. Сохраните внесенные изменения.

Действия с правилами доступа к веб-ресурсам

Не рекомендуется создавать более 1000 правил доступа к веб-ресурсам, поскольку это может привести к нестабильности системы.

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют точно задать круг веб-ресурсов, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- Фильтр по содержанию. Веб-Контроль разделяет веб-ресурсы по категориям содержания и категориям типа данных. Вы можете контролировать доступ пользователей к размещенным на веб-ресурсах данным, относящихся к определенными этими категориями типам данных. При посещении пользователями вебресурсов, которые относятся к выбранной категории содержания и / или категории типа данных, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет действие, указанное в правиле.

- Фильтр по адресам веб-ресурсов. Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

  Если задан и фильтр по содержанию, и фильтр по адресам веб-ресурсов, и заданные адреса вебресурсов и / или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типа данных, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и / или категорий типа данных, а только к заданным адресам вебресурсов и / или группам адресов веб-ресурсов.

- Фильтр по именам пользователей и групп пользователей. Вы можете задавать пользователей и / или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.

- Расписание работы правила. Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует доступ к веб-ресурсам, указанным в правиле.

После установки программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready список правил компонента Веб-Контроль не пуст. Предустановлены два правила:

- Правило "Сценарии и таблицы стилей", которое разрешает всем пользователям в любое время доступ к веб-ресурсам, адреса которых содержат названия файлов с расширением css, js, vbs. Например: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- "Правило по умолчанию". Это правило в зависимости от выбранного действия разрешает или запрещает всем пользователям доступ ко всем веб-ресурсам, которые не попадают под действие других правил.

Добавление и изменение правила доступа к веб-ресурсам

Чтобы добавить или изменить правило доступа к веб-ресурсам, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Веб-Контроль.

3. Выполните одно из следующих действий:

   - Если вы хотите добавить правило, нажмите на кнопку Добавить.

   - Если вы хотите изменить правило, выберите правило в таблице и нажмите на кнопку Изменить.

   Откроется окно Правило доступа к веб-ресурсам.

4. Задайте или измените параметры правила. Для этого выполните следующие действия:

   a. В поле Название введите или измените название правила.

   b. В раскрывающемся списке Фильтровать содержание выберите нужный элемент:

      - Любое содержание.

      - По категориям содержания.

      - По типам данных.

      - По категориям содержания и типам данных.

   c. Если выбран элемент, отличный от Любое содержание, откроются блоки для выбора категорий содержания и / или типов данных. Установите флажки напротив названий желаемых категорий содержания и / или типов данных.

      Установка флажка напротив названия категории содержания и / или типа данных означает, что Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, в соответствии с правилом, контролирует доступ к веб-ресурсам, принадлежащим к выбранным категориям содержания и / или типам данных.

   d. В раскрывающемся списке Применять к адресам выберите нужный элемент:

      - Ко всем адресам.

      - К отдельным адресам.

e. Если выбран элемент К отдельным адресам, откроется блок, в котором требуется создать список адресов веб-ресурсов. Вы можете добавлять или изменять адреса и / или группы адресов вебресурсов, используя кнопки Добавить, Изменить, Удалить.

> Если Проверка защищенных соединений отключена, для протокола https доступна фильтрация только по имени сервера.

f. В раскрывающемся списке Применять к адресам выберите нужный элемент:

- Ко всем пользователям.
- К отдельным пользователям или группам.

g. Если выбран элемент К отдельным пользователям или группам, откроется блок, в котором вы можете создать список пользователей и / или групп пользователей, доступ которых к веб-ресурсам, описанным в правиле, регулируется этим правилом. Вы можете добавлять или удалять пользователей и / или группы пользователей, используя кнопки Добавить, Удалить.

По кнопке Добавить открывается стандартное окно Microsoft Windows Выбор пользователей или групп.

h. Из раскрывающегося списка Действие выберите нужный элемент:

- Разрешать. Если выбрано это значение, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает доступ к вебресурсам, удовлетворяющим параметрам правила.
- Запрещать. Если выбрано это значение, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запрещает доступ к вебресурсам, удовлетворяющим параметрам правила.
- Предупреждать. Если выбрано это значение, то при попытке доступа к веб-ресурсам, удовлетворяющим правилу, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выводит предупреждение о том, что вебресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

i. Выберите из раскрывающегося списка Расписание работы правила название нужного расписания или сформируйте новое расписание на основе выбранного расписания работы правила. Для этого выполните следующие действия:

1. Нажмите на кнопку Настройка напротив раскрывающегося списка Расписание работы правила.

   Откроется окно Расписание работы правила.

2. Чтобы добавить в расписание работы правила интервал времени, в течение которого правило не работает, в таблице с изображением расписания работы правила левой клавишей мыши выберите ячейки таблицы, соответствующие нужному вам времени и дню недели.

   Цвет ячеек изменится на серый.

3. Чтобы в расписании работы правила изменить интервал времени, в течение которого правило работает, на интервал времени, в течение которого правило не работает, левой клавишей мыши выберите серые ячейки таблицы, соответствующие нужному вам времени и дню недели.

   Цвет ячеек изменится на зеленый.

4. Нажмите на кнопку Сохранить как.

   Откроется окно Название расписания работы правила.

5. Введите название расписания работы правила или оставьте название, предложенное по умолчанию.

6. Нажмите на кнопку OK.

5. Сохраните внесенные изменения.

Назначение приоритета правилам доступа к веб-ресурсам

Вы можете назначить приоритет каждому правилу из списка правил, расположив их в определенном порядке.

Чтобы назначить правилам доступа к веб-ресурсам приоритет, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Веб-Контроль.
3. В правой части окна выберите правило, приоритет которого вы хотите изменить.
4. С помощью кнопок Вверх и Вниз переместите правило на желаемую позицию в списке правил.
5. Повторите действие пунктов инструкции 3-4 для тех правил, приоритет которых вы хотите изменить.
6. Сохраните внесенные изменения.

Проверка работы правил доступа к веб-ресурсам

Чтобы оценить, насколько согласованы правила Веб-Контроля, вы можете проверить их работу. Для этого в рамках компонента Веб-Контроль предусмотрена функция "Диагностика правил".

Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Веб-Контроль.
3. В правой части окна нажмите на кнопку Диагностика.

   Откроется окно Диагностика правил.

4. Заполните поля в блоке Условия:

   a. Установите флажок Укажите адрес, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует доступ к определенному веб-ресурсу. В поле ниже введите адрес веб-ресурса.

b. Задайте список пользователей и / или групп пользователей, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует доступ к веб-ресурсам для определенных пользователей и / или групп пользователей.

c. Из раскрывающегося списка Фильтровать содержание выберите нужный элемент (По категориям содержания, По типам данных или По категориям содержания и типам данных), если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует доступ к веб-ресурсам определенных категорий содержания и / или категорий типа данных.

d. Установите флажок Учитывать время попытки доступа, если вы хотите проверить работу правил с учетом дня недели и времени совершения попытки доступа к веб-ресурсам, указанным в условиях диагностики правил. Далее укажите день недели и время.

5. Нажмите на кнопку Проверить.

В результате проверки выводится сообщение о действии Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в соответствии с первым сработавшим правилом при попытке доступа к заданному веб-ресурсу (разрешение, запрет, предупреждение). Первым срабатывает правило, которое находится в списке правил Веб-Контроля выше других правил, удовлетворяющих условиям диагностики. Сообщение выводится справа от кнопки Проверить. В таблице ниже выводится список остальных сработавших правил с указанием действия, которое выполняет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Правила выводятся в порядке убывания приоритета.

Включение и выключение правила доступа к веб-ресурсам

Чтобы включить или выключить правило доступа к веб-ресурсам, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Веб-Контроль.

3. В правой части окна выберите правило, которое вы хотите включить или выключить.

4. В графе Статус выполните следующие действия:

- Если вы хотите включить использование правила, выберите значение Вкл.

- Если вы хотите выключить использование правила, выберите значение Выкл.

.

5 Сохраните внесенные изменения.

Миграция правил доступа к веб-ресурсам из предыдущих версий программы

При обновлении программы с версии Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 10 Service Pack 2 для Windows и с более ранних версий до Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11.4.0 для Windows правила доступа к веб-ресурсам, основанные на категориях содержания веб-ресурсов, мигрируют по следующим правилам:

- Правила доступа к веб-ресурсам, основанные на одной или нескольких категориях содержания вебресурсов из списка "Чаты и форумы", "Веб-почта", "Социальные сети", становятся основанными на категории содержания веб-ресурсов "Общение в сети".
- Правила доступа к веб-ресурсам, основанные на одной или нескольких категориях содержания вебресурсов из списка "Интернет-магазины" и "Платежные системы", становятся основанными на категории содержания веб-ресурсов "Интернет-магазины, банки, платежные системы".
- Правила доступа к веб-ресурсам, основанные на категории содержания веб-ресурсов "Азартные игры", становятся основанными на категории содержания веб-ресурсов "Азартные игры, лотереи, тотализаторы".
- Правила доступа к веб-ресурсам, основанные на категории содержания веб-ресурсов "Браузерные игры", становятся основанными на категории содержания веб-ресурсов "Компьютерные игры".
- Правила доступа к веб-ресурсам, основанные на категориях содержания веб-ресурсов, не перечисленных в предыдущих пунктах списка, мигрируют без изменений.

Экспорт и импорт списка адресов веб-ресурсов

Если в правиле доступа к веб-ресурсам вы сформировали список адресов веб-ресурсов, вы можете экспортировать его в файл формата TXT. В дальнейшем вы можете импортировать список из этого файла, чтобы при настройке правила не создавать список адресов веб-ресурсов вручную. Возможность экспорта и импорта списка адресов веб-ресурсов может понадобиться, например, если вы создаете правила со сходными параметрами.

Чтобы экспортировать список адресов веб-ресурсов в файл, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Веб-Контроль.
3. Выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать в файл.
4. Нажмите на кнопку Изменить.

   Откроется окно Правило доступа к веб-ресурсам.

.

5. Если вы хотите экспортировать не весь список адресов веб-ресурсов, а только его часть, выделите нужные вам адреса веб-ресурсов.

6. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

   Откроется окно подтверждения действия.

7 Выполните одно из следующих действий:

- Если вы хотите экспортировать только выделенные элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку Да.
- Если вы хотите экспортировать все элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку Нет.

  Откроется стандартное окно Microsoft Windows Сохранить как.

8. В окне Microsoft Windows Сохранить как выберите файл, в который вы хотите экспортировать список адресов веб-ресурсов, и нажмите на кнопку Сохранить.

Чтобы импортировать в правило список адресов веб-ресурсов из файла, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Веб-Контроль.

3. Выполните одно из следующих действий:

- Нажмите на кнопку Добавить, если вы хотите создать новое правило доступа к веб-ресурсам.
- Выберите правило доступа к веб-ресурсам, которое вы хотите изменить. Далее нажмите на кнопку Изменить.

   Откроется окно Правило доступа к веб-ресурсам.

4. Выполните одно из следующих действий:

- Если вы создаете новое правило доступа к веб-ресурсам, в раскрывающемся списке Применять к адресам выберите элемент К отдельным адресам.
- Если вы изменяете правило доступа к веб-ресурсам, перейдите к пункту 5 инструкции.

5. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

   Если вы создаете новое правило, откроется стандартное окно Microsoft Windows Открыть файл.

   Если вы изменяете правило, откроется окно подтверждения действия.

6. Выполните одно из следующих действий:

- Если вы создаете новое правило доступа к веб-ресурсам, перейдите к пункту 7 инструкции.
- Если вы изменяете правило доступа к веб-ресурсам, в окне подтверждения действия выполните одно из следующих действий:

- Если вы хотите добавить к существующим импортируемые элементы списка адресов веб-ресурсов, нажмите на кнопку Да.
- Если вы хотите удалить существующие элементы списка адресов веб-ресурсов и добавить импортируемые, нажмите на кнопку Нет.

Откроется стандартное окно Microsoft Windows Открыть файл.

7. В окне Microsoft Windows Открыть файл выберите файл со списком адресов веб-ресурсов для импорта.
8. Нажмите на кнопку Открыть.
9. В окне Правило доступа к веб-ресурсам нажмите на кнопку OK.

Мониторинг активности пользователей в интернете

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет записывать данные о посещении пользователями всех веб-сайтов, в том числе и разрешенных. Таким образом, вы можете получить полную историю просмотров в браузере. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправляет события активности пользователя в Kaspersky Security Center, локальный журнал Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, журнал событий Windows. Для получения событий в Kaspersky Security Center нужно настроить параметры событий в политике в Консоли администрирования или Web Console. Также вы можете настроить отправку событий Веб-Контроля по электронной почте и отображение уведомлений на экране компьютера пользователя.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает следующие события активности пользователя в интернете:

- блокировка веб-сайта (статус Критические события ); посещение
- нерекомендованного веб-сайта (статус Предупреждения ); посещение
- разрешенного веб-сайта (статус Информационные сообщения ).

Чтобы настроить запись событий Веб-Контроля на компьютере пользователя, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Интерфейс.
3. В блоке Уведомления нажмите на кнопку Настройка.
4. В открывшемся окне выберите раздел Веб-Контроль.

   Откроется таблица событий Веб-Контроля и способов уведомлений.

.

5. Настройте для каждого события способ уведомления: Сохранять в локальном журнале и Сохранять в журнале событий Windows.

   Для записи событий посещения разрешенных веб-сайтов нужно дополнительно настроить Веб-Контроль (см. инструкцию ниже).

   Также в таблице событий вы можете включить уведомление на экране и уведомление по электронной почте. Для отправки уведомлений по почте нужно настроить параметры SMTP-сервера. Подробнее об отправке уведомлений по почте см. в справке Kaspersky Security Center.

6. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready начинает записывать события активности пользователя в интернете.

Веб-Контроль отправляет события активности пользователя в Kaspersky Security Center следующим образом:

- Если вы используете Kaspersky Security Center, Веб-Контроль отправляет события по всем объектам, из которых состоит веб-страница. Поэтому при блокировании одной веб-страницы может быть создано несколько событий. Например, при блокировании веб-страницы http://www.example.com Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может отправить события по следующим объектам: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/ le.js и так далее.

- Если вы используете Kaspersky Security Center Cloud Console, Веб-Контроль группирует события и отправляет только протокол и домен веб-сайта. Например, если пользователь посетил нерекомендованные веб-страницы http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправит только одно событие с объектом http://www.example.com.

Чтобы включить запись событий посещения разрешенных веб-сайтов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Веб-Контроль.

3. Нажмите на кнопку Дополнительные параметры.

4. В открывшемся окне установите флажок Записывать данные о посещении разрешенных страниц в журнал.

5. Сохраните внесенные изменения.

В результате вам будет доступна полная история просмотров в браузере.

Правила формирования масок адресов веб-ресурсов

Использование маски адреса веб-ресурса (далее также "маски адреса") может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам требуется ввести множество схожих адресов вебресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса следует использовать следующие правила:

1. Символ `*` заменяет любую последовательность из нуля или более символов.

   Например, при вводе маски адреса `*abc*` правило доступа к веб-ресурсам применяется ко всем адресам, содержащим последовательность `abc`. Пример: `http://www.example.com/page_09abcdef.html`.

   Для включения символа `*` в состав маски адреса требуется вводить два символа `*`.

2. Последовательность символов `www.` в начале маски адреса трактуется как последовательность `*.`.

   Пример: маска адреса `www.example.com` трактуется как `*.example.com`.

3. Если маска адреса начинается не с символа `*`, то содержание маски адреса эквивалентно тому же содержанию с префиксом `*.`.

.

4. Последовательность символов `*.` в начале маски трактуется как `*.` или пустая строка.

   Пример: под действие маски адреса `http://www.*.example.com` попадает адрес `http://www2.example.com`.

5 Если маска адреса заканчивается символом, отличным от `/` или `*`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

   Пример: под действие маски адреса `http://www.example.com` попадают адреса вида `http://www.example.com/abc`, где a, b, c – любые символы.

6. Если маска адреса заканчивается символом `/`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

7. Последовательность символов `/*` в конце маски адреса трактуется как `/*` или пустая строка.

8. Проверка адресов веб-ресурсов по маске адреса осуществляется с учетом схемы (http или https):

   - Если сетевой протокол в маске адреса отсутствует, то под действие маски адреса попадает адрес с любым сетевым протоколом.

     Пример: под действие маски адреса `example.com` попадают адреса `http://example.com` и `https://example.com`.

   - Если сетевой протокол в маске адреса присутствует, то под действие маски адреса попадают только адреса с таким же сетевым протоколом, как у маски адреса.

     Пример: под действие маски адреса `http://*.example.com` попадает адрес `http://www.example.com` и не попадает адрес `https://www.example.com`.

9. Маска адреса, заключенная в двойные кавычки, трактуется без учета каких-либо дополнительных подстановок, за исключением символа `*`, если он изначально включен в состав маски адреса. Для масок адреса, заключенных в двойные кавычки, не выполняются правила 5 и 7 (см. примеры 14 – 18 в таблице ниже).

10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Примеры применения правил формирования масок адресов

№	Маска адреса	Проверяемый адрес вебресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
1	*.example.com	http://www.123example.com	Нет	См. правило 1.
2	*.example.com	http://www.123.example.com	Да	См. правило 1.
3	*example.com	http://www.123example.com	Да	См. правило 1.
4	*example.com	http://www.123.example.com	Да	См. правило 1.
5	http://www.*.example.com	http://www.123example.com	Нет	См. правило 1.

6	www.example.com	http://www.example.com	Да	См. правила 2, 1.
7	www.example.com	https://www.example.com	Да	См. правила 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 2, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	"example.com"	http://www.example.com	Нет	См. правило 9.
15	"http://www.example.com"	http://www.example.com/abc	Нет	См. правило 9.
16	"*.example.com"	http://www.example.com	Да	См. правила 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Да	См. правила 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше информации, чем адрес вебресурса.

Изменение шаблонов сообщений Веб-Контроля

В зависимости от действия, заданного в свойствах правил Веб-Контроля, при попытке пользователей получить доступ к веб-ресурсам Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выводит сообщение (подменяет ответ HTTPсервера HTML-страницей с сообщением) одного из следующих типов:

- Сообщение-предупреждение. Такое сообщение предупреждает пользователя о том, что посещение вебресурса не рекомендуется и / или не соответствует корпоративной политике безопасности. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выводит сообщение-предупреждение, если в параметрах правила, описывающего этот веб-ресурс, в раскрывающемся списке Действие выбран элемент Предупреждать.

.

Если, по мнению пользователя, предупреждение ошибочно, по ссылке из предупреждения пользователь может отправить уже сформированное сообщение администратору локальной сети организации.

- Сообщение о блокировке веб-ресурса. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выводит сообщение о блокировке веб-ресурса, если в параметрах правила, которое описывает этот веб-ресурс, в раскрывающемся списке Действие выбран элемент Запрещать.

  Если блокировка доступа к веб-ресурсу, по мнению пользователя, была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения для отправки администратору локальной сети организации предусмотрены шаблоны. Вы можете изменять их содержание.

Чтобы изменить шаблон сообщений Веб-Контроля, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Веб-Контроль.
3. В правой части окна нажмите на кнопку Шаблоны.

   Откроется окно Шаблоны сообщений.

4 Выполните одно из следующих действий:

   - Если вы хотите изменить шаблон сообщения для пользователя о том, что веб-ресурс не рекомендован для посещения, выберите закладку Предупреждение.
   - Если вы хотите изменить шаблон сообщения о блокировке доступа к веб-ресурсу, выберите закладку Блокировка.
   - Если вы хотите изменить шаблон сообщения администратору, выберите закладку Сообщение администратору.

5. Измените шаблон сообщения. При этом вы можете использовать раскрывающийся список Переменная, а также кнопки По умолчанию и Ссылка (кнопка не доступна на закладке Сообщение администратору).
6. Сохраните внесенные изменения.

Адаптивный контроль аномалий

Компонент Адаптивный контроль аномалий доступен только для продуктов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для бизнеса Расширенный и Kaspersky Total Security для бизнеса (более подробная информация о продуктах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для бизнеса доступна на сайте "Лаборатории Касперского").

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Адаптивный контроль аномалий отслеживает и блокирует действия, нехарактерные для компьютеров сети организации. Для отслеживания нехарактерных действий Адаптивный контроль аномалий использует набор правил (например, правило Запуск Windows PowerShell из офисной программы). Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил и, например, разрешить запуск PowerShell-скриптов для автоматизации решения корпоративных задач. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обновляет набор правил с базами программы. Обновление набора правил нужно подтверждать вручную.

Настройка Адаптивного контроля аномалий

Настройка Адаптивного контроля аномалий состоит из следующих этапов:

1. Обучение Адаптивного контроля аномалий.

   После включения Адаптивного контроля аномалий правила работают в обучающем режиме. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил и отправляет события срабатывания в Kaspersky Security Center. Каждое правило имеет свой срок действия обучающего режима. Срок действия обучающего режима устанавливают специалисты "Лаборатории Касперского". Обычно срок действия обучающего режима составляет 2 недели.

   Если в ходе обучения правило ни разу не сработало, Адаптивный контроль аномалий будет считать действия, связанные с этим правилом, нехарактерными. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет блокировать все действия, связанные с этим правилом.

   Если в ходе обучения правило сработало, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready регистрирует события в отчете о срабатываниях правил и в хранилище Срабатывание правил в обучающем режиме.

.

2. Анализ отчета о срабатывании правил.

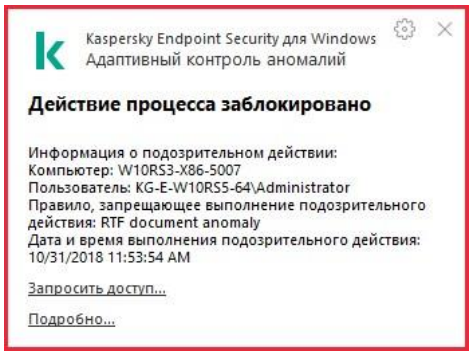
   Администратор анализирует отчет о срабатываниях правил или содержание хранилища Срабатывание правил в обучающем режиме. Далее администратор может выбрать поведение Адаптивного контроля аномалий при срабатывании правила: блокировать или разрешить. Также администратор может продолжить отслеживать срабатывание правила и продлить работу программы в обучающем режиме. Если администратор не предпринимает никаких мер, программа также продолжит работать в обучающем режиме. Отсчет срока действия обучающего режима начинается заново.

Настройка Адаптивного контроля аномалий происходит в режиме реального времени. Настройка Адаптивного контроля аномалий осуществляется по следующим каналам:

- Адаптивный контроль аномалий автоматически начинает блокировать действия, связанные с правилами, которые не сработали в течение обучающего режима.
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавляет новые правила или удаляет неактуальные.
-

Администратор настраивает работу Адаптивного контроля аномалий после анализа отчета о срабатывании правил и содержимого хранилища Срабатывание правил в обучающем режиме.
Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища Срабатывание правил в обучающем режиме.

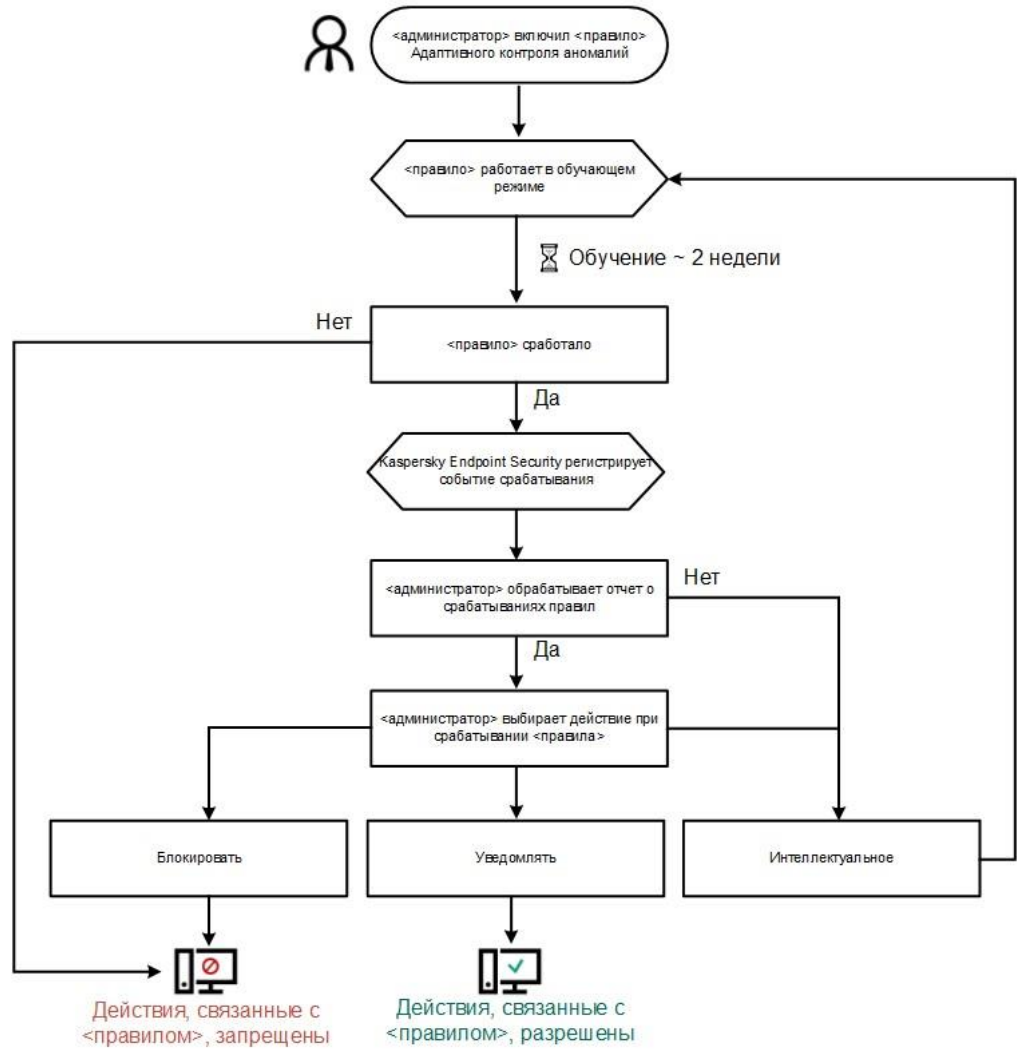
При попытке вредоносной программы выполнить действие, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует действие и покажет уведомление (см. рис. ниже).



Уведомление Адаптивного контроля аномалий

Алгоритм работы Адаптивного контроля аномалий

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready принимает решение о выполнении действия, связанного с правилом, по следующему алгоритму (см. рис. ниже).



Алгоритм работы Адаптивного контроля аномалий

Включение и выключение Адаптивного контроля аномалий

По умолчанию Адаптивный контроль аномалий включен.

Чтобы включить или выключить Адаптивный контроль аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Адаптивный контроль аномалий.
3. Выполните одно из следующих действий:
   - Установите флажок Адаптивный контроль аномалий, если вы хотите включить Адаптивный контроль аномалий.
   - Снимите флажок Адаптивный контроль аномалий, если вы хотите выключить Адаптивный контроль аномалий.

4. Сохраните внесенные изменения.

Включение и выключение правила Адаптивного контроля аномалий

Чтобы включить или выключить правило Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Адаптивный контроль аномалий.
3. В таблице в правой части окна выберите правило.
4. В графе Статус по правой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:
   - Включено. Статус означает, что правило используется во время работы компонента Адаптивный контроль аномалий.
   - Выключено. Статус означает, что правило не используется во время работы компонента Адаптивный контроль аномалий.
5. Сохраните внесенные изменения.

Изменение действия при срабатывании правила Адаптивного контроля аномалий

Чтобы изменить действие при срабатывании правила Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Адаптивный контроль аномалий.
3. В таблице в правой части окна выберите правило.
4. В графе Действие по правой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:
   - Интеллектуальное. Если выбран этот вариант, то правило Адаптивного контроля аномалий работает в обучающем режиме в течение периода, определенного специалистами "Лаборатории Касперского". В этом режиме при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает активность, подпадающую под это правило, и создает запись в хранилище Срабатывание правил в обучающем режиме Сервера администрирования Kaspersky Security Center. По истечении периода работы обучающего режима Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует активность, подпадающую под правило Адаптивного контроля аномалий, и создает в журнале запись, содержащую информацию об этой активности.

- Блокировать. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.

- Информировать. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.

5. Сохраните внесенные изменения.

Создание и изменение исключения для правила Адаптивного контроля аномалий

Для правил Адаптивного контроля аномалий невозможно создать более 1000 исключений. Не рекомендуется создавать более 200 исключений. Чтобы уменьшить количество используемых исключений, рекомендуется использовать маски в параметрах исключений.

Исключение для правила Адаптивного контроля аномалий включает в себя описание исходных и целевых объектов. Исходный объект – объект, который выполняет действия. Целевой объект – объект, над которым выполняются действия. Например, вы открыли файл `file.xlsx`. В результате в память компьютера была добавлена библиотека с расширением dll, которую использует браузер (исполняемый файл `browser.exe`). В данном примере `file.xlsx` – исходный объект, Excel – исходный процесс, `browser.exe` – целевой объект, Browser – целевой процесс.

Чтобы создать или изменить исключение для правила Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Адаптивный контроль аномалий.

3. В таблице в правой части окна выберите правило.

4. Нажмите на кнопку Изменить.

   Откроется окно Правило Адаптивного контроля аномалий.

5. Выполните одно из следующих действий:

   - Если вы хотите добавить исключение, нажмите на кнопку Добавить.

   - Если вы хотите изменить существующее исключение, выберите строку в таблице Исключения и нажмите на кнопку Изменить.

   Откроется окно Исключение из правила.

6. В поле Описание введите описание исключения.

7. Нажмите на кнопку Обзор рядом с полем Пользователь, чтобы указать пользователей, на которых распространяется исключение.

   Откроется стандартное окно Microsoft Windows Выбор пользователей или групп.

8. Задайте параметры исходного объекта или исходного процесса, запущенных объектом:

   - Исходный процесс. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`).
   - Хеш исходного процесса. Хеш файла.
   - Исходный объект. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`). Например, путь к файлу `document.docm`, который запускает целевые процессы с помощью скрипта или макроса.

     Вы также можете указать другие объекты для исключения, например, веб-адрес, макрос, команду в командной строке, путь реестра и другие. Укажите объект по следующему шаблону: `object://<объект>`, где `<объект>` – название объекта, например, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`.
     Вы также можете использовать маски, например, `object://*C:\Windows\temp\*`.

   - Хеш исходного объекта. Хеш файла.

   Правило Адаптивного контроля аномалий не распространяется на действия, выполняемые объектом, или на процессы, запущенные объектом.

9. Задайте параметры целевого объекта или целевых процессов, запущенных над объектом.

   - Целевой процесс. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`).
   - Хеш целевого процесса. Хеш файла.
   - Целевой объект. Команда запуска целевого процесса. Укажите команду по следующему шаблону `object://<команда>`, например, `object://cmdline:powershell -Command "$result = 'C:\windows\temp\result_local_users_pwdage.txt'"`. Также вы можете использовать маски, например, `object://*C:\windows\temp\*`.
   - Хеш целевого объекта. Хеш файла.

   Правило Адаптивного контроля аномалий не распространяется на действия над объектом или на процессы, запущенные над объектом.

10. Сохраните внесенные изменения.

Удаление исключения для правила Адаптивного контроля аномалий

Чтобы удалить исключение для правила Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Адаптивный контроль аномалий.
3. В таблице в правой части окна выберите правило.
4. Нажмите на кнопку Изменить.

   Откроется окно Правило Адаптивного контроля аномалий.
5. В таблице Исключения из правила выберите нужную строку.
6. Нажмите на кнопку Удалить.
7. Сохраните внесенные изменения.

Импорт исключений для правил Адаптивного контроля аномалий

Чтобы импортировать исключения для правил Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Адаптивный контроль аномалий.
3. Нажмите на кнопку Импорт.

   Откроется окно Выбор конфигурационного файла.
4. В окне Выбор конфигурационного файла укажите файл формата XML, из которого вы хотите импортировать список исключений.
5. Нажмите на кнопку Открыть.
6. Подтвердите импорт исключений по кнопке Да.
7. Сохраните внесенные изменения.

Экспорт исключений для правил Адаптивного контроля аномалий

Чтобы экспортировать исключения для выбранных правил, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Адаптивный контроль аномалий.
3. В таблице в правой части окна выберите одно или несколько правил, исключения для которых вы хотите экспортировать.

4. Нажмите на кнопку Экспорт.

   Откроется окно Выбор конфигурационного файла.

5. В окне Выбор конфигурационного файла выполните следующие действия:

   a. Укажите имя файла формата XML, в который вы хотите экспортировать исключения.

   b. Выберите папку, в которой вы хотите сохранить этот файл.

   c. Нажмите на кнопку Сохранить.

6. В открывшемся диалоговом окне выполните одно из следующих действий:

   - Нажмите на кнопку Да, если вы хотите экспортировать исключения только для выбранных правил.
   - Нажмите на кнопку Нет, если вы хотите экспортировать исключения для всех правил.

7. Сохраните внесенные изменения.

Применение обновлений для правил Адаптивного контроля аномалий

Новые правила Адаптивного контроля аномалий могут быть добавлены в таблицу правил и существующие правила Адаптивного контроля аномалий могут быть удалены из таблицы правил по результату обновления антивирусных баз. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выделяет удаляемые и добавляемые правила Адаптивного контроля аномалий в таблице, если для этих правил обновление не было применено.

До тех пор, пока обновление не применено, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображает удаленные в результате обновления правила Адаптивного контроля аномалий в таблице правил и присваивает этим правилам статус Выключено. Изменение параметров этих правил невозможно.

Чтобы применить обновления для правил Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Контроль безопасности → Адаптивный контроль аномалий.

3. Нажмите на кнопку Подтвердить обновления.

   Кнопка Подтвердить обновления доступна, если доступно обновление для правил Адаптивного контроля аномалий.

4. Сохраните внесенные изменения.

Изменение шаблонов сообщений Адаптивного контроля аномалий

Когда пользователь пытается выполнить действие, запрещенное правилами Адаптивного контроля аномалий, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выводит сообщение о блокировке потенциально опасных действий. Если блокировка, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации.

Для сообщения о блокировке потенциально опасных действий и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

Чтобы изменить шаблон сообщения, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Контроль безопасности → Адаптивный контроль аномалий.
3. Установите флажок Адаптивный контроль аномалий, чтобы параметры компонента стали доступными для изменения.
4. Нажмите на кнопку Шаблоны.

   Откроется окно Шаблоны сообщений.
5. Выполните одно из следующих действий:

   - Если вы хотите изменить шаблон сообщения о блокировке потенциально опасных действий, выберите закладку Блокировка.
   - Если вы хотите изменить шаблон сообщения для администратора локальной сети организации, выберите закладку Сообщение администратору.
6. Измените шаблон сообщения о блокировке или сообщения администратору.
7. Сохраните внесенные изменения.

Просмотр отчетов Адаптивного контроля аномалий

Чтобы просмотреть отчеты Адаптивного контроля аномалий, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В разделе Контроль безопасности выберите подраздел Адаптивный контроль аномалий.

   В правой части окна отобразятся параметры компонента Адаптивный контроль аномалий.

6. Выполните одно из следующих действий:

   - Если вы хотите просмотреть отчет о параметрах правил Адаптивного контроля аномалий, нажмите на кнопку Отчет о состоянии правил.
   - Если вы хотите просмотреть отчет о срабатываниях правил Адаптивного контроля аномалий, нажмите на кнопку Отчет о срабатываниях правил.

7. Запустится процесс формирования отчета.

Отчет отобразится в новом окне.

Контроль сетевых портов

Во время работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready компоненты Веб-Контроль, Защита от почтовых угроз, Защита от веб-угроз контролируют потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP- и UDP-порты компьютера пользователя. Например, компонент Защита от почтовых угроз анализирует информацию, передаваемую по SMTP-протоколу, а компонент Защита от вебугроз анализирует информацию, передаваемую по протоколам HTTP и FTP.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready подразделяет TCP- и UDP-порты компьютера пользователя на несколько групп в соответствии с вероятностью их взлома. Сетевые порты, отведенные для уязвимых служб, рекомендуется контролировать более тщательно, так как эти сетевые порты с большей вероятностью могут являться целью сетевой атаки. Если вы используете нестандартные службы, которым отведены нестандартные сетевые порты, эти сетевые порты также могут являться целью для атакующего компьютера. Вы можете задать список сетевых портов и список программ, запрашивающих сетевой доступ, на которые компоненты Защита от почтовых угроз и Защита от веб-угроз должны обращать особое внимание во время слежения за сетевым трафиком.

Включение контроля всех сетевых портов

Чтобы включить контроль всех сетевых портов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры сети.
3. В блоке Контролируемые порты выберите вариант Контролировать все сетевые порты.
4. Сохраните внесенные изменения.

Включение контроля портов для программ из списка, сформированного специалистами "Лаборатории Касперского"

Чтобы сформировать список контролируемых сетевых портов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры сети.
3. В блоке Контролируемые порты выберите вариант Контролировать только выбранные сетевые порты.
4. Нажмите на кнопку Настройка.

   Откроется окно Сетевые порты.
5. Установите флажок Контролировать все порты для программ из списка, рекомендованного "Лабораторией Касперского".

   Если установлен этот флажок, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует все порты для следующих программ:

   - Adobe Reader.
   - AIM for Windows.
   - Apple Application Support.
   - Chrome.
   - Digsby.

- Edge.
- Firefox.
- Google Talk.
- ICQ.
- Internet Explorer.
- Java.
- Mail.ru Агент.
- Miranda IM.
- mIRC.
- Opera.
- Pidgin.
- QIP In um.
- QIP.
- QNext.
- QNextClient.
- Rockmelt.
- Safari.
- Simple Instant Messenger.
- Trillian.
- Windows Live Messenger.
- Windows Messenger.
- X-Chat.
- Yahoo! Messenger.
- Яндекс.Браузер.

Формирование списка контролируемых сетевых портов

Чтобы сформировать список контролируемых сетевых портов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры сети.
3. В блоке Контролируемые порты выберите вариант Контролировать только выбранные сетевые порты.
4. Нажмите на кнопку Настройка.

   Откроется окно Сетевые порты. В окне Сетевые порты находится список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика. Этот список сетевых портов включен в поставку Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
5. В списке сетевых портов выполните следующие действия:

   - Установите флажки напротив названий тех сетевых портов, которые вы хотите включить в список контролируемых сетевых портов.

     По умолчанию флажки установлены для всех сетевых портов, представленных в окне Сетевые порты.
   - Снимите флажки напротив названий тех сетевых портов, которые вы хотите исключить из списка контролируемых сетевых портов.
6. Если сетевой порт отсутствует в списке сетевых портов, добавьте его следующим образом:

   a. По ссылке Добавить, расположенной под списком сетевых портов, откройте окно Сетевой порт. b. В поле Порт введите номер сетевого порта.

   c. В поле Описание введите название сетевого порта.

   d. Нажмите на кнопку ОК.

   Окно Сетевой порт закроется. Добавленный вами сетевой порт отобразится в конце списка сетевых портов.
7. Сохраните внесенные изменения.

При работе протокола FTP в пассивном режиме соединение может устанавливаться через случайный сетевой порт, который не добавлен в список контролируемых сетевых портов. Чтобы защищать такие соединения, требуется установить флажок Контролировать все сетевые порты в блоке Контролируемые порты или настроить контроль всех сетевых портов для программ, с помощью которых устанавливается FTP-соединение.

Формирование списка программ, для которых контролируются все сетевые порты

Вы можете сформировать список программ, для которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует все сетевые порты.

В список программ, для которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует все сетевые порты, рекомендуется включить программы, которые принимают или передают данные по протоколу FTP.

Чтобы сформировать список программ, для которых контролируются все сетевые порты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры сети.
3. В блоке Контролируемые порты выберите вариант Контролировать только выбранные сетевые порты.
4. Нажмите на кнопку Настройка.

   Откроется окно Сетевые порты.
5. Установите флажок Контролировать все порты для указанных программ.
6. В списке программ, расположенном под флажком Контролировать все порты для указанных программ, выполните следующие действия:

   - Установите флажки напротив названий программ, для которых нужно контролировать все сетевые порты.

     По умолчанию флажки установлены для всех программ, представленных в окне Сетевые порты.
   - Снимите флажки напротив названий программ, для которых не нужно контролировать все сетевые порты.
7. Если программа отсутствует в списке программ, добавьте ее следующим образом:

   a. По ссылке Добавить, расположенной под списком программ, откройте контекстное меню.

   b. Выберите в контекстном меню способ добавления программы в список программ:

      - Выберите пункт Программы, если вы хотите выбрать программу из списка программ, установленных на компьютере. Откроется окно Выбор программы, с помощью которого вы можете указать название программы.
      - Выберите пункт Обзор, если вы хотите указать местонахождение исполняемого файла программы. Откроется стандартное окно Microsoft Windows Открыть, с помощью которого вы можете указать название исполняемого файла программы.

     После выбора программы откроется окно Программа.

   c. В поле Название введите название для выбранной программы.

   d. Нажмите на кнопку ОК.

     Окно Программа закроется. Добавленная вами программа отобразится в конце списка программ.
8. Сохраните внесенные изменения.

Удаление данных

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет дистанционно удалять данные на компьютерах пользователей с помощью задачи.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет данные следующим образом:

- в тихом режиме; на жестких и съемных
- дисках; для всех учетных записей на
- компьютере.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет задачу Удаление данных при любом типе лицензирования, даже после истечения срока действия лицензии.

Режимы удаления данных

Задача позволяет удалять данные в следующих режимах:

- Немедленное удаление данных.

  В этом режиме вы можете, например, удалить устаревшие данные, чтобы освободить дисковое пространство.

- Отложенное удаление данных.

  Этот режим предназначен, например, для защиты данных на ноутбуке в случае его потери или кражи. Вы можете настроить автоматическое удаление данных, если ноутбук покинул пределы сети организации и давно не синхронизировался с Kaspersky Security Center.

Настроить расписание удаления данных в свойствах задачи невозможно. Вы можете только немедленно удалить данные после запуска задачи вручную или настроить отложенное удаление данных при отсутствии связи с Kaspersky Security Center.

Ограничения

Удаление данных имеет следующие ограничения:

- Управление задачей Удаление данных доступно только администратору Kaspersky Security Center. Настроить или запустить задачу в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready невозможно.
- Для файловой системы NTFS Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет имена только основных потоков данных. Удалить имена альтернативных потоков данных невозможно.
- При удалении файла символической ссылки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready также удаляет файлы, пути к которым указаны в символической ссылке.

Создание задачи удаления данных

Чтобы удалить данные на компьютерах пользователей, выполните следующие действия:

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Добавить.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке Программа выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).

   b. В раскрывающемся списке Тип задачи выберите Удаление данных.

   c. В поле Название задачи введите короткое описание, например, `Удаление данных (Анти-Вор)`.

   d. В блоке Выбор устройств, которым будет назначена задача выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку Далее.

   Если в группу администрирования области действия задачи добавлены новые компьютеры, то задача немедленного удаления данных запускается на новых компьютерах только при условии, что между завершением выполнения задачи и добавлением новых компьютеров прошло менее 5 минут.

5. Завершите работу мастера по кнопке Готово.

   В списке задач отобразится новая задача.

6. Нажмите на задачу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready Удаление данных.

   Откроется окно свойств задачи.

7. Выберите закладку Параметры программы.

8. Выберите метод удаления данных:

   - Удалять средствами операционной системы. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет файлы средствами операционной системы без помещения файлов в корзину.

   - Удалять без возможности восстановления. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready перезаписывает файлы случайными данными. Восстановить данные после удаления практически невозможно.

9. Если вы хотите использовать отложенное удаление данных, установите флажок Автоматически удалять данные при отсутствии связи с Kaspersky Security Center более N дней. Задайте количество дней.

Задача в режиме отложенного удаления данных будет выполняться при каждом превышении срока отсутствия связи с Kaspersky Security Center.

При настройке отложенного удаления данных учитывайте, что сотрудники могут, например, выключить компьютер перед уходом в отпуск. В этом случае срок отсутствия связи может быть превышен и данные будут удалены. Также учитывайте график работы автономных пользователей. Подробнее о работе с автономными компьютерами и автономными пользователями см. в справке Kaspersky Security Center.

Если флажок снят, задача будет выполнена сразу после синхронизации с Kaspersky Security Center.

10. Создайте список объектов для удаления:

- Папки. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready удалит все файлы в папке, а также вложенные папки. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не поддерживает маски и переменные окружения при вводе пути к папке.

- Файлы по расширению. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready выполнит поиск файлов с указанными расширениями на всех дисках компьютера, в том числе съемных дисках. Для указания нескольких расширений используйте символы ";" или ",".

- Стандартные области. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready удалит файлы из следующих областей:

Документы. Файлы в стандартной папке операционной системы Документы, а также вложенные папки.

- Файлы Cookies. Файлы, в которых браузер сохраняет данные с посещенных пользователем вебсайтов (например, данные для авторизации пользователя).

- Рабочий стол. Файлы в стандартной папке операционной системы Рабочий стол, а также вложенные папки.

- Временные файлы Internet Explorer. Временные файлы, связанные с работой браузера Internet Explorer: копии веб-страниц, изображений и медиафайлов.

- Временные файлы. Временные файлы, связанные с работой установленных на компьютере программ. Например, программы Microsoft O ice создают временные файлы с резервными копиями документов.

- Файлы Outlook. Файлы, связанные с работой почтового клиента Outlook: файлы данных (PST), автономные файлы данных (OST), файлы автономной адресной книги (OAB) и файлы персональной адресной книги (PAB).

- Профиль пользователя. Набор файлов и папок, в которых хранятся параметры операционной системы для учетной записи локального пользователя.

Вы можете создать список объектов для удаления на каждой из закладок. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready создаст общий консолидированный список и удалит файлы из этого списка при выполнении задачи.

Удалить файлы, необходимые для работы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, невозможно.

11. Нажмите на кнопку Сохранить.

12. Установите флажок напротив задачи.

13. Нажмите на кнопку Запустить.

В результате на компьютерах пользователей будут удалены данные в соответствии с выбранным режимом: немедленно или при отсутствии связи. Если Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не может удалить файл, например, пользователь использует файл в настоящий момент, программа не пытается удалить его снова. Для завершения удаления данных повторите запуск задачи.

Защита паролем

Для версии программы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Windows 11.1.0 и выше порядок работы Защиты паролем изменился. В Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Windows 11.1.0 вы можете ограничить доступ к программе отдельным пользователям и не использовать одну учетную запись. При обновлении с предыдущих версий программы, если Защита паролем включена, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready сохраняет ранее заданный пароль. Для первого изменения параметров Защиты паролем используйте имя пользователя KLAdmin и ранее заданный пароль.

Компьютер могут использовать несколько пользователей с разным уровнем компьютерной грамотности. Неограниченный доступ пользователей к Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и его параметрам может привести к снижению уровня безопасности компьютера в целом. Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в соответствии с предоставленными разрешениями (например, разрешение на завершение работы программы).

Если пользователь, который запустил сессию Windows, (сессионный пользователь) имеет разрешение на выполнение действия, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не запрашивает имя пользователя и пароль или временный пароль. Пользователь получает доступ к Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в соответствии с предоставленными разрешениями.

Если у сессионного пользователя отсутствует разрешение на выполнение действия, пользователь может получить доступ к программе следующими способами:

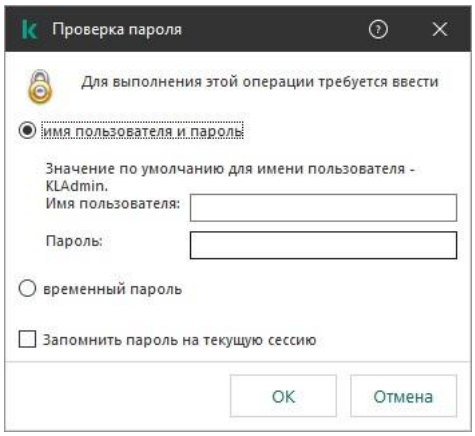
- Ввод имени пользователя и пароля.

  Этот способ удобен для повседневной работы. Для выполнения действия, защищенного паролем, требуется ввести данные доменной учетной записи пользователя с необходимым разрешением. При этом компьютер должен быть в домене. Если компьютер не в домене, вы можете использовать учетную запить KLAdmin.

- Ввод временного пароля.

  Этот способ удобен, если пользователь находится вне корпоративной сети и необходимо предоставить ему временное разрешение на выполнение запрещенного действия (например, завершить работу программы). По истечении срока действия временного пароля или истечении сессии программа возвращает параметры Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в прежнее состояние.

При попытке пользователя выполнить действие, защищенное паролем, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready предложит пользователю ввести имя пользователя и пароль или временный пароль (см. рис. ниже).



Запрос пароля для доступа к Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready

Имя пользователя и пароль

Для доступа к Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready необходимо ввести данные доменной учетной записи. Защита паролем поддерживает работу со следующими учетными записями:

- KLAdmin. Учетная запись администратора без ограничений доступа к Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем. Отменить разрешение для учетной записи KLAdmin невозможно. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready требует задать пароль для учетной записи KLAdmin во время включения Защиты паролем.

- Группа "Все". Стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети. Пользователи из группы "Все" могут получить доступ к программе в соответствии с предоставленными разрешениями.

- Отдельные пользователи или группы. Учетные записи пользователей, для которых вы можете настроить отдельные разрешения. Например, если для группы "Все" выполнение действия запрещено, то вы можете разрешить выполнение действия для отдельного пользователя или группы.

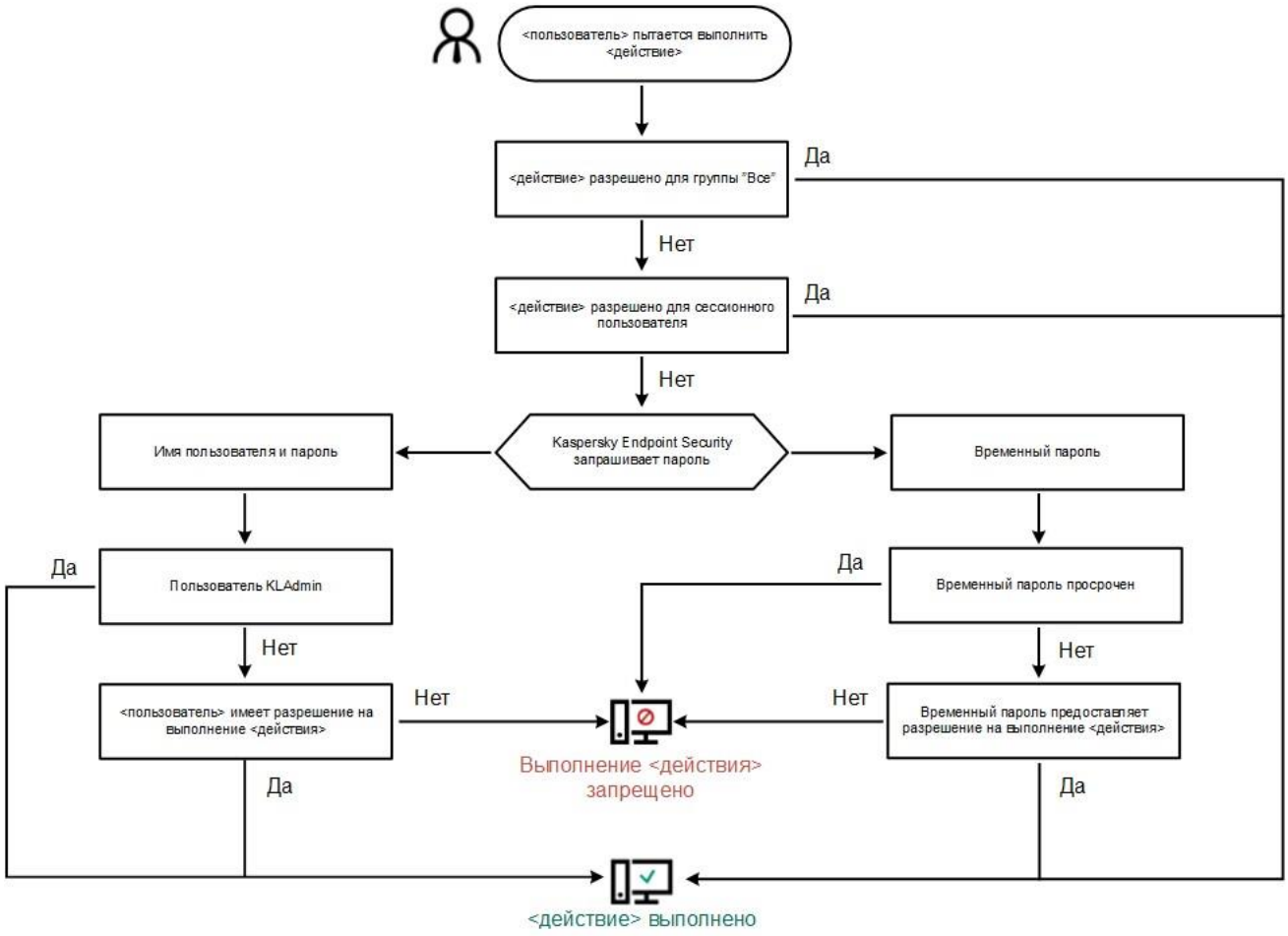
- Сессионный пользователь. Учетная запись пользователя, который запустил сессию Windows. Вы можете сменить сессионного пользователя во время ввода пароля (флажок Запомнить пароль на текущую сессию). В этом случае Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready назначает сессионным пользователем, учетные данные которого вы ввели, вместо пользователя, который запустил сессию Windows.

Временный пароль

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для отдельного компьютера вне корпоративной сети. Администратор создает временный пароль для отдельного компьютера в Kaspersky Security Center в свойствах компьютера пользователя. Администратор выбирает действия, на которые будет распространяться временный пароль, и срок действия временного пароля.

Алгоритм работы Защиты паролем

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready принимает решение о выполнении действия, защищенного паролем, по следующему алгоритму (см. рис. ниже).



Алгоритм работы Защиты паролем

Включение Защиты паролем

Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в соответствии с предоставленными разрешениями (например, разрешение на завершение работы программы).

Чтобы включить Защиту паролем, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Интерфейс.
3. В блоке Защита паролем нажмите на кнопку Настройка.

   Откроется окно Защита паролем.
4. В открывшемся окне установите флажок Включить защиту паролем.

5. Задайте пароль для учетной записи KLAdmin:

   a. В таблице Разрешения откройте список разрешений для учетной записи KLAdmin двойным щелчком мыши.

      Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем.

   b. В открывшемся окне нажмите на кнопку Пароль.

   c. Задайте пароль для учетной записи KLAdmin и подтвердите его.

   d. Нажмите на кнопку OK.

   Если компьютер работает под управлением политики, администратор может сбросить пароль для учетной записи KLAdmin в свойствах политики. Если компьютер не подключен к Kaspersky Security Center и вы забыли пароль для учетной записи KLAdmin, восстановить пароль невозможно.

6. Настройте разрешения для всех пользователей внутри корпоративной сети:

   a. В таблице Разрешения откройте список разрешений для группы "Все" двойным щелчком мыши.

      Группа "Все" – стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети.

   b. Установите флажки напротив тех действий, которые будут доступны пользователям без ввода пароля.

      Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения Завершение работы программы снят, вы можете завершить работу программы только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением или с помощью временного пароля.

      Разрешения Защиты паролем имеют ряд особенностей. Убедитесь, что для доступа к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполнены все условия.

   c. Нажмите на кнопку OK.

7. Сохраните внесенные изменения.

После включения Защиты паролем программа ограничит доступ пользователей к Kaspersky Endpoint Security в соответствии в разрешениями для группы "Все". Вы можете выполнить запрещенные для группы "Все" действия только с помощью учетной записи KLAdmin, отдельной учетной записи с нужными разрешениями или с помощью временного пароля.

Вы можете выключить Защиту паролем только с помощью учетной записи KLAdmin. Выключить защиту паролем с помощью другой учетной записи или с помощью временного пароля невозможно.

Во время проверки пароля вы можете установить флажок Запомнить пароль на текущую сессию. В этом случае Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не будет требовать ввода пароля при попытке пользователя выполнить другое разрешенное действие, защищенное паролем, в течение сессии.

Предоставление разрешений для отдельных пользователей или групп

Вы можете предоставить доступ к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для отдельных пользователей или групп. Например, если группе "Все" запрещено завершать работу программы, вы можете предоставить отдельному пользователю разрешение Завершение работы программы. В результате вы можете завершить работу программы только с помощью учетной записи этого пользователя или учетной записи KLAdmin.

Вы можете использовать данные учетной записи для доступа к программе, только если компьютер в домене. Если компьютер не в домене, вы можете использовать учетную запить KLAdmin или временный пароль.

Чтобы предоставить разрешение для отдельных пользователей или групп, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Интерфейс.
3. В блоке Защита паролем нажмите на кнопку Настройка.

   Откроется окно Защита паролем.
4. В таблице Разрешения нажмите на кнопку Добавить.

   Откроется окно Разрешения пользователя/группы.
5. Справа от поля Пользователь/Группа нажмите на кнопку Выбрать.

   Откроется стандартное окно Windows для выбора пользователей или групп.
6. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.
7. В таблице Разрешения установите флажки напротив тех действий, которые будут доступны добавленному пользователю или группе без ввода пароля.

   Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения Завершение работы программы снят, вы можете завершить работу программы только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением или с помощью временного пароля.

   Разрешения Защиты паролем имеют ряд особенностей. Убедитесь, что для доступа к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполнены все условия.
8. Сохраните внесенные изменения.

В результате, если для группы "Все" доступ к программе ограничен, пользователи получат доступ к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в соответствии с разрешениями для этих пользователей.

Использование временного пароля для предоставления разрешений

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для отдельного компьютера вне корпоративной сети. Это нужно, чтобы разрешить выполнение запрещенного действия без передачи пользователю учетных данных KLAdmin. Для использования временного пароля компьютер должен быть добавлен в Kaspersky Security Center.

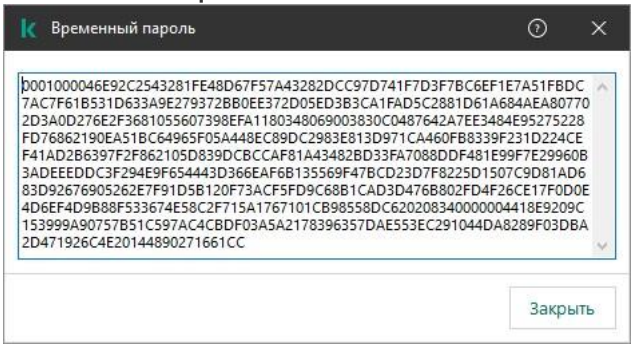
Чтобы предоставить пользователю разрешение на выполнение запрещенного действия с помощью временного пароля, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Устройства.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел Программы.
6. В списке установленных на компьютере программ "Лаборатории Касперского" выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows и откройте свойства программы двойным щелчком мыши.
7. В окне параметров программы выберите раздел Общие параметры → Интерфейс.
8. В блоке Защита паролем нажмите на кнопку Настройка.

   Откроется окно Защита паролем.
9. В блоке Временный пароль нажмите на кнопку Настройка.

   Откроется окно Создание временного пароля.
10. В поле Дата истечения установите срок действия временного пароля.
11. В таблице Область действия временного пароля установите флажки напротив тех действий, которые будут доступны пользователю после ввода временного пароля.
12. Нажмите на кнопку Создать.

    Откроется окно с временным паролем (см. рис. ниже).
13. Скопируйте и передайте пользователю пароль.



Временный пароль

Особенности разрешений Защиты паролем

Разрешения Защиты паролем имеют ряд особенностей и ограничений.

Настройка параметров программы

Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты открыты).

Завершение работы программы

Особенностей и ограничений нет.

Выключение компонентов защиты

- Предоставить разрешение на выключение компонентов защиты для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KLAdmin, но и другим пользователям, добавьте пользователя или группу с разрешением Выключение компонентов защиты в параметрах Защиты паролем.
- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты открыты).
- Для выключения компонентов защиты в параметрах программы пользователь должен иметь разрешение Настройка параметров программы.
- Для выключения компонентов защиты из контекстного меню (пункт Приостановка защиты и контроля) пользователь, кроме разрешения Выключение компонентов защиты, должен иметь разрешение Выключение компонентов контроля.

Выключение компонентов контроля

- Предоставить разрешение на выключение компонентов контроля для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KLAdmin, но и другим пользователям, добавьте пользователя или группу с разрешением Выключение компонентов контроля в параметрах Защиты паролем.
- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты открыты).
- Для выключения компонентов контроля в параметрах программы пользователь должен иметь разрешение Настройка параметров программы.
- Для выключения компонентов контроля из контекстного меню (пункт Приостановка защиты и контроля) пользователь, кроме разрешения Выключение компонентов контроля, должен обладать разрешением Выключение компонентов защиты.

Выключение политики Kaspersky Security Center

Предоставить разрешение на выключение политики Kaspersky Security Center для группы "Все" невозможно. Чтобы разрешить выключение политики не только пользователю KLAdmin, но и другим пользователям, добавьте пользователя или группу с разрешением Выключение политики Kaspersky Security Center в параметрах Защиты паролем.

Удаление ключа

Особенностей и ограничений нет.

Удаление / изменение / восстановление программы

Особенностей и ограничений нет.

Восстановление доступа к данным на зашифрованных устройствах

Вы можете восстановить доступ к данным на зашифрованных устройствах только с помощью учетной записи KLAdmin. Разрешить это действие другому пользователю невозможно.

Просмотр отчетов

Особенностей и ограничений нет.

Восстановление из резервного хранилища

Особенностей и ограничений нет.

Доверенная зона

Доверенная зона – это сформированный администратором системы список объектов и программ, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не контролирует в процессе работы. Иначе говоря, это набор исключений из проверки.

Доверенную зону администратор системы формирует самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от программ, установленных на компьютере. Включение объектов и программ в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что этот объект или программа безвредны.

Вы можете исключать из проверки объекты следующими способами:

- укажите путь к файлу или
- папке; введите хеш объекта;
- используйте маски:
  - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске C, но не в подпапках.
  - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам).

    Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папке `Folder` и вложенных папках. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
  - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.
- введите название объекта по классификации Вирусной энциклопедии "Лаборатории Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

Исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет объект на вирусы и другие программы, представляющие угрозу.

Исключения из проверки позволяют работать с легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского".

В результате работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready такие программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ вы

можете настроить исключения из проверки. Для этого нужно добавить в доверенную зону название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского". Например, вы часто используете в своей работе программу Radmin, предназначенную для удаленного управления компьютерами. Такая активность программы рассматривается Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready как подозрительная и может быть заблокирована. Чтобы исключить блокировку программы, нужно сформировать исключение из проверки, где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

Если у вас на компьютере установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из проверки, настроив Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready способом, описанным в этом документе.

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач программы, заданных администратором системы:

- Анализ поведения.
- Защита от эксплойтов.
- Предотвращение вторжений.
- Защита от файловых угроз.
- Защита от веб-угроз.
- Защита от почтовых угроз.
- Задачи проверки.

Список доверенных программ

Список доверенных программ – это список программ, у которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не контролирует файловую и сетевую активность (в том числе и вредоносную), а также обращения этих программ к системному реестру. По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready исключает из проверки программу, добавленную в список доверенных программ.

Например, если вы считаете объекты, используемые программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, вам следует добавить программу Microsoft Windows Блокнот в список доверенных программ, чтобы не проверять объекты, используемые этой программой.

Кроме того, некоторые действия, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда программ. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных программ.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и другой антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

В то же время исполняемый файл и процесс доверенной программы по-прежнему проверяются на наличие в них вирусов и других программ, представляющих угрозу. Для полного исключения программы из проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready следует пользоваться исключениями из проверки.

Создание исключения из проверки

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет объект, если при запуске одной из задач проверки в область проверки включен диск, на котором находится объект, или папка, в которой находится объект. Однако при запуске задачи выборочной проверки именно для этого объекта исключение из проверки не применяется.

Чтобы создать исключение из проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Исключения.
3. В блоке Исключения из проверки и доверенные программы нажмите на кнопку Настройка.
4. В открывшемся окне установите флажок Объединять значения при наследовании, если вы хотите создать общий список исключений из проверки для всех компьютеров организации.

   Списки исключений из проверки родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Исключения из проверки родительской политики отображаются в дочерних политиках и доступны только для просмотра.
   Изменение или удаление исключений из проверки родительской политики невозможно.
5. Нажмите на кнопку Добавить.

   Откроется окно Исключение из проверки. В этом окне вы можете сформировать исключение из проверки, используя один или оба критерия из блока Свойства.
6. Если вы хотите исключить из проверки файл или папку, выполните следующие действия:

   a. В блоке Свойства установите флажок Файл или папка.

   b. По ссылке выберите файл или папку, расположенной в блоке Описание исключения из проверки, откройте окно Имя файла или папки.

   c. Введите имя файла или папки, маску имени файла или папки или выберите файл или папку в дереве папок, нажав на кнопку Обзор.

      Используйте маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске C, но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением `txt` в папке `Folder` и вложенных папках. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

В маске имени файла или папки вы можете использовать символ *, который заменяет любой набор символов в имени файла.

Например, вы можете использовать маски для добавления следующих путей:

- Пути к файлам, расположенным в любой из папок:
  - Маска `*.exe` будет включать все пути к файлам с расширением exe.
  - Маска `example*` будет включать все пути к файлам с именем EXAMPLE.
- Пути к файлам, расположенным в указанной папке:
  - маска `C:\dir\*.*` будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
  - маска `C:\dir\*` будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\; маска `C:\dir\` будет включать все пути к файлам в папке C:\dir\, но не в подпапках
  - папки C:\dir\;
  - маска `C:\dir\*.exe` будет включать все пути к файлам с расширением exe в папке C:\dir\, но не в подпапках папки C:\dir\;
  - маска `C:\dir\test` будет включать все пути к файлам с именем test в папке C:\dir\, но не в подпапках папки C:\dir\;
  - маска `C:\dir\*\test` будет включать все пути к файлам с именем test в папке C:\dir\ и в подпапках папки C:\dir\.
- Пути к файлам, расположенным во всех папках с указанным именем:
  - маска `dir\*.*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
  - маска `dir\*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;

- маска `dir\` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\*.exe` будет включать все пути к файлам с расширением exe в папках с именем dir, но не в подпапках этих папок;
- маска `dir\test` будет включать все пути к файлам с именем test в папках с именем dir, но не в подпапках этих папок.

d. Нажмите на кнопку OK в окне Имя файла или папки.

Ссылка на добавленный файл или папку появится в блоке Описание исключения из проверки окна Исключение из проверки.

7. Если вы хотите исключить из проверки объекты с определенным названием, выполните следующие действия:

a. В блоке Свойства установите флажок Название объекта.

b. По ссылке введите название объекта, расположенной в блоке Описание исключения из проверки, откройте окно Название объекта.

c. Введите название или маску названия объекта согласно классификации Вирусной энциклопедии "Лаборатории Касперского".

d. Нажмите на кнопку OK в окне Название объекта.

Ссылка на добавленное название объекта появится в блоке Описание исключения из проверки окна Исключение из проверки.

8. Если необходимо, в поле Комментарий введите краткий комментарий к создаваемому исключению из проверки.

9. Определите компоненты Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, в работе которых должно быть использовано исключение из проверки:

a. По ссылке любые, расположенной в блоке Описание исключения из проверки, активируйте ссылку выберите компоненты.

b. По ссылке выберите компоненты откройте окно Компоненты защиты.

c. Установите флажки напротив тех компонентов, на работу которых должно распространяться исключение из проверки.

d. Нажмите на кнопку OK в окне Компоненты защиты.

Если компоненты указаны в параметрах исключения из проверки, то исключение применяется при проверке только этими компонентами Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

Если компоненты не указаны в параметрах исключения из проверки, то исключение применяется при проверке всеми компонентами Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

10. Нажмите на кнопку OK в окне Исключение из проверки.

Добавленное исключение из проверки появится в таблице на закладке Исключения из проверки окна Доверенная зона. В блоке Описание исключения из проверки отобразятся заданные параметры этого исключения из проверки.

11. Сохраните внесенные изменения.

Изменение исключения из проверки

Чтобы изменить исключение из проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Исключения.
3. В блоке Исключения из проверки и доверенные программы нажмите на кнопку Настройка.

   Откроется окно Доверенная зона на закладке Исключения из проверки.
4. В списке выберите нужное исключение из проверки.
5. Измените параметры исключения из проверки одним из следующих способов:

   - Нажмите на кнопку Изменить.

     Откроется окно Исключения из проверки.

   - Откройте окно для изменения нужного параметра по ссылке в поле Описание исключения из проверки.
6. Если на предыдущем шаге вы нажали на кнопку Изменить, нажмите на кнопку OK в окне Исключение из проверки.

   В блоке Описание исключения из проверки отобразятся измененные параметры исключения из проверки.
7. Сохраните внесенные изменения.

Удаление исключения из проверки

Чтобы удалить исключение из проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Исключения.
3. В блоке Исключения из проверки и доверенные программы нажмите на кнопку Настройка.

   Откроется окно Доверенная зона на закладке Исключения из проверки.
4. В списке исключений из проверки выберите нужное исключение из проверки.
5. Нажмите на кнопку Удалить.

   Удаленное исключение из проверки исчезнет из списка.
6. Сохраните внесенные изменения.

Запуск и остановка работы исключения из проверки

Чтобы запустить или остановить работу исключения из проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Исключения.
3. В блоке Исключения из проверки и доверенные программы нажмите на кнопку Настройка.

   Откроется окно Доверенная зона на закладке Исключения из проверки.
4. В списке исключений из проверки выберите нужное исключение.
5. Выполните одно из следующих действий:

   - Установите флажок рядом с названием исключения из проверки, если вы хотите запустить работу этого исключения.
   - Снимите флажок рядом с названием исключения из проверки, если вы хотите временно приостановить работу этого исключения.
6. Сохраните внесенные изменения.

Формирование списка доверенных программ

Чтобы сформировать список доверенных программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Исключения.
3. В блоке Исключения из проверки и доверенные программы нажмите на кнопку Настройка.

   Откроется окно Доверенная зона.
4. В окне Доверенная зона выберите закладку Доверенные программы.
5. В открывшемся окне установите флажок Объединять значения при наследовании, если вы хотите создать общий список доверенных программ для всех компьютеров организации.

   Списки доверенных программ родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные программы родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных программ родительской политики невозможно.
6. Если вы хотите добавить программу в список доверенных программ, выполните следующие действия: a.

   Нажмите на кнопку Добавить.

   b. В раскрывшемся контекстном меню выполните одно из следующих действий:

- Выберите пункт Программы, если вы хотите найти программу в списке установленных на компьютере программ.

  Откроется окно Выбор программы.

- Выберите пункт Обзор, если вы хотите указать путь к исполняемому файлу нужной программы.

  Откроется стандартное окно Microsoft Windows Открыть.

c. Выберите программу одним из следующих способов:

- Если на предыдущем шаге вы выбрали пункт Программы, выберите программу в списке установленных на компьютере программ и нажмите на кнопку OK в окне Выбор программы.

- Если на предыдущем шаге вы выбрали пункт Обзор, укажите путь к исполняемому файлу нужной программы и нажмите на кнопку Открыть в стандартном окне Microsoft Windows Открыть.

В результате выполненных действий откроется окно Исключения из проверки для программы.

d. Установите флажки напротив нужных правил доверенной зоны для выбранной программы:

- Не проверять открываемые файлы.
- Не контролировать активность программы.
- Не наследовать ограничения родительского процесса (программы).
- Не контролировать активность дочерних программ.
- Не блокировать взаимодействие с интерфейсом программы.
- Не блокировать взаимодействие с Поставщиком AMSI-защиты.
- Не проверять сетевой трафик.

e. Нажмите на кнопку OK в окне Исключения из проверки для программы.

В списке доверенных программ появится добавленная доверенная программа.

7. Если вы хотите изменить параметры доверенной программы, выполните следующие действия:

a. Выберите доверенную программу из списка доверенных программ.

b. Нажмите на кнопку Изменить.

c. Откроется окно Исключения из проверки для программы.

d. Установите или снимите флажки напротив нужных правил доверенной зоны для выбранной программы.

> Если в окне Исключения из проверки для программы не выбрано ни одно из правил доверенной зоны для программы, то происходит включение доверенной программы в проверку. Доверенная программа не удаляется из списка доверенных программ, но флажок для нее снимается.

e. Нажмите на кнопку OK в окне Исключения из проверки для программы.

8. Если вы хотите удалить доверенную программу из списка доверенных программ, выполните следующие действия:

   a. Выберите доверенную программу из списка доверенных программ.

   b. Нажмите на кнопку Удалить.

9. Сохраните внесенные изменения.

Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ

Чтобы включить или выключить действие правил доверенной зоны на программу из списка доверенных программ, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Исключения.
3. В блоке Исключения из проверки и доверенные программы нажмите на кнопку Настройка.

   Откроется окно Доверенная зона.
4. В окне Доверенная зона выберите закладку Доверенные программы.
5. В списке доверенных программ выберите нужную доверенную программу.
6. Выполните одно из следующих действий:

   - Установите флажок рядом с названием доверенной программы, если хотите выключить ее из проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
   - Снимите флажок рядом с названием доверенной программы, если хотите включить ее в проверку Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
7. Сохраните внесенные изменения.

Использование доверенного системного хранилища сертификатов

Использование системного хранилища сертификатов позволяет исключать из антивирусной проверки программы, подписанные доверенной цифровой подписью.

Чтобы начать использовать доверенное системное хранилище сертификатов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Исключения.

3. В блоке Исключения из проверки и доверенные программы нажмите на кнопку Настройка.

   Откроется окно Доверенная зона.

4. В окне Доверенная зона выберите закладку Доверенное системное хранилище сертификатов.

5. Установите флажок Использовать доверенное системное хранилище сертификатов.

6. В раскрывающемся списке Доверенное системное хранилище сертификатов выберите, какое системное хранилище Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready должен считать доверенным.

7. Сохраните внесенные изменения.

Работа с резервным хранилищем

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. Резервная копия – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

В Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете попытаться восстановить файл из его резервной копии в папку исходного размещения файла.

Если Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready работает под управлением Kaspersky Security Center, то резервные копии файлов могут быть передана на Сервер администрирования Kaspersky Security Center. Подробнее о работе резервными копиями файлов в Kaspersky Security Center можно прочитать в Справочной системе Kaspersky Security Center.

Настройка максимального срока хранения файлов в резервном хранилище

По умолчанию максимальный срок хранения копий файлов в резервном хранилище составляет 30 дней. По истечении максимального срока хранения Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет наиболее старые файлы из резервного хранилища. Вы можете отменить ограничение по времени или изменить максимальный срок хранения файлов.

Чтобы настроить максимальный срок хранения файлов в резервном хранилище, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Отчеты и хранение.

3. Выполните одно из следующих действий:

   - В правой части окна в блоке Резервное хранилище установите флажок Хранить объекты не более, если хотите ограничить срок хранения копий файлов в резервном хранилище. В поле справа от флажка Хранить объекты не более укажите максимальный срок хранения копий файлов в резервном хранилище. По умолчанию максимальный срок хранения копий файлов в резервном хранилище составляет 30 дней.

   - В правой части окна в блоке Резервное хранилище снимите флажок Хранить объекты не более, если хотите отменить ограничение срока хранения копий файлов в резервном хранилище.

4. Сохраните внесенные изменения.

Настройка максимального размера резервного хранилища

По умолчанию максимальный размер резервного хранилища составляет 100 МБ. После достижения максимального размера Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически удаляет наиболее старые файлы из резервного хранилища таким образом, чтобы не превышался его максимальный размер. Вы можете отменить ограничение на максимальный размер резервного хранилища или изменить максимальный размер.

Чтобы настроить максимальный размер резервного хранилища, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Отчеты и хранение.

3. Выполните одно из следующих действий:

   - Если вы хотите ограничить суммарный размер резервного хранилища, установите флажок Максимальный размер хранилища в правой части окна в блоке Резервное хранилище и укажите максимальный размер резервного хранилища в поле справа от флажка Максимальный размер хранилища.

     По умолчанию максимальный размер хранилища данных, включающего в себя резервные копии файлов, составляет 100 МБ.

   - Если вы хотите отменить ограничение на размер резервного хранилища, снимите флажок Максимальный размер хранилища в правой части окна в блоке Резервное хранилище.

   По умолчанию размер резервного хранилища не ограничен.

4. Сохраните внесенные изменения.

Восстановление файлов из резервного хранилища

Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует файл, присваивает ему статус Заражен, помещает его копию в резервное хранилище и пытается провести лечение. Если файл удается вылечить, то статус резервной копии файла изменяется на Вылечен. Файл становится доступен в папке исходного размещения. Если файл не удается вылечить, то

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready удаляет его из папки исходного размещения. Вы можете восстановить файл из его резервной копии в папку исходного размещения.

Файлы со статусом Будет вылечен при перезагрузке компьютера восстановить невозможно. Перезагрузите компьютер и статус файла изменится на Вылечен или Удален. При этом вы можете восстановить файл из его резервной копии в папку исходного размещения.

В случае обнаружения вредоносного кода в файле, который является частью приложения Windows Store, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не помещает копию файла в резервное хранилище, а сразу удаляет его. При этом восстановить целостность приложения Windows Store вы можете средствами операционной системы Microsoft Windows 8 (подробную информацию о восстановлении приложения Windows Store читайте в Справочной системе к Microsoft Windows 8).

Набор резервных копий файлов представлен в виде таблицы. Для резервной копии файла отображается путь к папке исходного размещения этого файла. Путь к папке исходного размещения файла может содержать персональные данные.

Вы можете скопировать информацию о выбранных файлах резервного хранилища в буфер обмена. Чтобы выбрать несколько файлов резервного хранилища, откройте по правой клавише мыши контекстное меню любого файла и выберите пункт Выделить все. Далее отметьте те файлы, с которых вы хотите снять выделение, удерживая клавишу CTRL.

Если в резервное хранилище помещено несколько расположенных в одной и той же папке файлов с одинаковыми именами и различным содержимым, то для восстановление доступен только тот файл, который был помещен в резервное хранилище последним.

Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:

1. В главном окне программ нажмите на кнопку Хранилища.

   Откроется окно Резервное хранилище.

2. Если вы хотите восстановить все файлы из резервного хранилища, то в окне Резервное хранилище в контекстном меню любого файла выберите пункт Восстановить все.

   Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready восстановит все файлы из их резервных копий в папки их исходного размещения.

3. Если вы хотите восстановить один или несколько файлов из резервного хранилища, то выполните следующие действия:

   a. В таблице в окне Резервное хранилище выберите один или несколько файлов резервного хранилища.

      Чтобы выбрать несколько файлов резервного хранилища, откройте по правой клавише мыши контекстное меню любого файла и выберите пункт Выделить все. Далее отметьте те файлы, с которых вы хотите снять выделение, удерживая клавишу CTRL.

   b. Восстановите файлы одним из следующих способов:

      - Нажмите на кнопку Восстановить.
      - По правой клавише мыши откройте контекстное меню и выберите пункт Восстановить.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready восстановит файлы из выбранных резервных копий в папки их исходного размещения.

Удаление резервных копий файлов из резервного хранилища

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет резервные копии файлов с любым статусом из резервного хранилища автоматически по истечении времени, заданного в параметрах программы. Также вы можете самостоятельно удалить любую копию файла из резервного хранилища.

Чтобы удалить резервные копии файлов из резервного хранилища, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Хранилища.
2. Откроется окно Резервное хранилище.
3. Если вы хотите удалить все файлы из резервного хранилища, то выполните одно из следующих действий:
   - В контекстном меню любого файла выберите пункт Удалить все.
   - Нажмите на кнопку Очистить хранилище.

   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удалит все резервные копии файлов из резервного хранилища.
4. Если вы хотите удалить один или несколько файлов из резервного хранилища, то выполните следующие действия:
   a. В таблице в окне Резервное хранилище выберите один или несколько файлов резервного хранилища.

      Чтобы выбрать несколько файлов резервного хранилища, откройте по правой клавише мыши контекстное меню любого файла и выберите пункт Выделить все. Далее отметьте те файлы, с которых вы хотите снять выделение, удерживая клавишу CTRL.

   b. Нажмите на кнопку Удалить.

   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удалит выбранные резервные копии файлов из резервного хранилища.

Служба уведомлений

В процессе работы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready возникают различного рода события. Уведомления об этих событиях могут иметь информационный характер или нести важную информацию. Например, уведомление может информировать об успешно выполненном обновлении баз и модулей программы, а может фиксировать ошибку в работе некоторого компонента, которую вам требуется устранить.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready позволяет вносить информацию о событиях, возникающих в работе программы, в журнал событий Microsoft Windows и / или в журнал Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready может доставлять уведомления следующими способами:

- с помощью всплывающих уведомлений в области уведомлений панели задач Microsoft
- Windows; по электронной почте.

Вы можете настроить способы доставки уведомлений. Способ доставки уведомлений устанавливается для каждого типа событий.

Вы можете выполнить следующие действия для настройки службы уведомлений:

- настроить параметры журналов событий, где Kaspersky Endpoint Security для бизнеса –
- Расширенный EDR Ready сохраняет события; настроить отображение уведомлений на
- экране; настроить доставку уведомлений по электронной почте.

Работая с таблицей событий для настройки службы уведомлений, вы можете выполнять следующие действия:

- фильтровать события службы уведомлений по значениям граф или по условиям сложного
- фильтра; использовать функцию поиска событий службы уведомлений; сортировать события
- службы уведомлений; изменять порядок и набор граф, отображаемых в списке событий
- службы уведомлений.

Настройка параметров журналов событий

Чтобы настроить параметры журналов событий, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Интерфейс.
3. В блоке Уведомления нажмите на кнопку Настройка.

   Откроется окно Уведомления.

В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

События могут содержать следующие данные пользователя:

- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security для
- бизнеса - Расширенный EDR Ready; пути к ключам реестра, изменяемым в
- ходе работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR
- Ready; имя пользователя Microsoft Windows; адреса веб-страниц,

открываемых пользователем.

4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить параметры журналов событий.

5. В графах Сохранять в локальном отчете и Сохранять в журнале событий Windows установите флажки напротив нужных событий.

   События, напротив которых установлен флажок в графе Сохранять в локальном отчете, отображаются в Журналах приложений и служб в разделе Журнал событий Kaspersky. События, напротив которых установлен флажок в графе Сохранять в журнале событий Windows, отображаются в Журналах Windows в разделе Приложение. Чтобы открыть журналы событий, выберите Пуск → Панель управления → Администрирование → Просмотр событий.

6. Сохраните внесенные изменения.

Настройка отображения и доставки уведомлений

Чтобы настроить отображение и доставку уведомлений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Интерфейс.

3. В блоке Уведомления нажмите на кнопку Настройка.

   Откроется окно Уведомления.

   В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

   События могут содержать следующие данные пользователя:

   - пути к файлам, проверяемым с помощью Kaspersky Endpoint Security для
   - бизнеса - Расширенный EDR Ready; пути к ключам реестра, изменяемым в
   - ходе работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR
   -

Ready; имя пользователя Microsoft Windows; адреса веб-страниц,

открываемых пользователем.

4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить доставку уведомлений.

5. В графе Уведомлять на экране установите флажки напротив нужных событий.

   Информация о выбранных событиях отображается на экране в виде всплывающих уведомлений в области уведомлений панели задач Microsoft Windows.

6. В графе Уведомлять по почте установите флажки напротив нужных событий.

   Информация о выбранных событиях доставляется по электронной почте, если заданы параметры доставки почтовых уведомлений.

7. Нажмите на кнопку Настройка почтовых уведомлений.

   Откроется окно Настройка почтовых уведомлений.

8. Установите флажок Отправлять сообщения о событиях, чтобы включить доставку информации о событиях в работе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, отмеченных в графе Уведомлять по почте.

9. Укажите параметры доставки почтовых уведомлений.

10. Сохраните внесенные изменения.

Настройка отображения предупреждений о состоянии программы в области уведомлений

Чтобы настроить отображение предупреждений о состоянии программы в области уведомлений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Интерфейс.

3. В блоке Предупреждения установите флажки напротив тех категорий событий, уведомления о которых вы хотите видеть в области уведомлений Microsoft Windows.

4. Сохраните внесенные изменения.

При возникновении событий, относящихся к выбранным категориям, значок программы в области уведомлений будет меняться на или в зависимости от важности предупреждения.

Работа с отчетами

Информация о работе каждого компонента Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, о событиях шифрования данных, о выполнении каждой задачи проверки, задачи обновления и задачи проверки целостности, а также о работе программы в целом сохраняется в отчетах.

Отчеты хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\Report`.

Отчеты могут содержать следующие данные пользователя:

- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security для
- бизнеса - Расширенный EDR Ready; пути к ключам реестра, изменяемым в
- ходе работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR
- Ready; имя пользователя Microsoft Windows; адреса веб-страниц,

открываемых пользователем.

Данные в отчете представлены в виде таблицы. Каждая строка таблицы содержит информацию об отдельном событии, атрибуты события находятся в графах таблицы. Некоторые графы являются составными и содержат вложенные графы с дополнительными атрибутами. Чтобы просмотреть дополнительные атрибуты, нажмите на кнопку ⊞ рядом с названием графы. События, зарегистрированные в работе разных компонентов или при выполнении разных задач, имеют разный набор атрибутов.

Доступны следующие отчеты:

- Отчет Системный аудит. Содержит информацию о событиях, возникающих в процессе взаимодействия пользователя с программой, а также в ходе работы программы в целом и не относящихся к каким-либо отдельным компонентам или задачам Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
- Отчеты о работе компонентов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
- Отчеты о выполнении задач Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
- Отчет Шифрование данных. Содержит информацию о событиях, возникающих при шифровании и расшифровке данных.

В отчетах применяются следующие уровни важности событий:

Информационные сообщения. События справочного характера, как правило, не несущие важной информации.

Предупреждения. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Критические события. События критической важности, указывающие на проблемы в работе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready или на уязвимости в защите компьютера пользователя.

Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

- фильтровать список событий по различным критериям;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке;
- сортировать список событий по каждой графе отчета; отображать
- и скрывать сгруппированные с помощью фильтра события по

кнопке ⊞; изменять порядок и набор граф, отображаемых в отчете.

При необходимости вы можете сохранить сформированный отчет в текстовый файл. Также вы можете удалять информацию из отчетов по компонентам и задачам Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, объединенным в группы.

Если Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready работает под управлением Kaspersky Security Center, то информация о событиях может быть передана на Сервер администрирования Kaspersky Security Center (подробнее см. в справке Kaspersky Security Center).

Просмотр отчетов

Если для пользователя доступен просмотр отчетов, то для этого пользователя доступен просмотр всех событий, отраженных в отчетах.

Чтобы просмотреть отчеты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Отчеты.

   Откроется окно Отчеты.

2. В левой части окна Отчеты в списке компонентов и задач выберите компонент или задачу.

   В правой части окна отобразится отчет, содержащий список событий по результатам работы выбранного компонента или выбранной задачи Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Вы можете отсортировать события в отчете по значениям в ячейках одной из граф. По умолчанию события в отчете отсортированы по возрастанию значений в ячейках графы Дата события.

3. Если требуется просмотреть подробную информацию о событии, выберите в отчете нужное событие.

   В нижней части окна отобразится блок со сводной информацией о событии.

Настройка максимального срока хранения отчетов

По умолчанию максимальный срок хранения отчетов о событиях, фиксируемых Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready автоматически удаляет наиболее

старые записи из файла отчета. Вы можете отменить ограничение по времени или изменить максимальный срок хранения отчетов.

Чтобы настроить максимальный срок хранения отчетов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Отчеты и хранение.
3. В правой части окна в блоке Отчеты выполните одно из следующих действий:
   - Установите флажок Хранить отчеты не более, если хотите ограничить срок хранения отчетов. В поле справа от флажка Хранить отчеты не более укажите максимальный срок хранения отчетов.

     По умолчанию максимальный срок хранения отчетов составляет 30 дней.
   - Снимите флажок Хранить отчеты не более, если хотите отменить ограничение срока хранения отчетов.

   По умолчанию ограничение срока хранения отчетов включено.
4. Сохраните внесенные изменения.

Настройка максимального размера файла отчета

Вы можете указать максимальный размер файла, содержащего отчет. По умолчанию максимальный размер файла отчета составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически удаляет наиболее старые записи из файла отчета таким образом, чтобы не превышался максимальный размер файла отчета. Вы можете отменить ограничение на размер файла отчета или установить другое значение.

Чтобы настроить максимальный размер файла отчета, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Отчеты и хранение.
3. В правой части окна в блоке Отчеты выполните одно из следующих действий:
   - Установите флажок Максимальный размер файла, если хотите ограничить размер файла отчета. В поле справа от флажка Максимальный размер файла укажите максимальный размер файла отчета.

     По умолчанию ограничение размера файла отчета составляет 1024 МБ.
   - Снимите флажок Максимальный размера файла, если хотите отменить ограничение на размер файла отчета.

   По умолчанию ограничение размера файла отчета включено.
4. Сохраните внесенные изменения.

Сохранение отчета в файл

Пользователь сам несет ответственность за обеспечение безопасности информации из сохраненного в файл отчета и, в частности, за контроль и ограничение доступа к этой информации.

Сформированный отчет вы можете сохранить в файл текстового формата TXT или CSV.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет событие в отчет в том виде, в каком событие отображается на экране, то есть с тем же составом и с той же последовательностью атрибутов события.

Чтобы сохранить отчет в файл, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Отчеты.

   Откроется окно Отчеты.

2. В левой части окна Отчеты в списке компонентов и задач выберите компонент или задачу.

   В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

3. Если требуется, измените представление данных в отчете с помощью следующих способов:

   - фильтрация событий; поиск
   - событий; изменение
   - расположения граф;
   - сортировка событий.

4. Нажмите на кнопку Сохранить отчет, расположенную в верхней правой части окна.

   Откроется контекстное меню.

5. В контекстном меню выберите нужную кодировку для сохранения файла отчета: Сохранить в ANSI или Сохранить в Unicode.

6. В открывшемся окне Сохранить как укажите папку, в которую вы хотите сохранить файл отчета.

7. В поле Имя файла введите название файла отчета.

8. В поле Тип файла выберите нужный формат файла отчета: TXT или CSV.

9. Сохраните внесенные изменения.

Удаление информации из отчетов

Чтобы удалить информацию из отчетов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Отчеты и хранение.
3. В правой части окна в блоке Отчеты нажмите на кнопку Удалить отчеты.

   Откроется окно Удаление отчетов.
4. Установите флажки для тех отчетов, из которых вы хотите удалить информацию:

   - Все отчеты.
   - Отчет компонентов защиты. Содержит информацию о работе следующих компонентов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready:
     - Анализ поведения.
     - Защита от эксплойтов.
     - Предотвращение вторжений.
     - Защита от файловых угроз.
     - Защита от веб-угроз.
     - Защита от почтовых угроз.
     - Защита от сетевых угроз.
     - Защита от атак BadUSB.
     - Поставщик AMSI-защиты.
   - Отчет компонентов контроля. Содержит информацию о работе следующих компонентов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready:
     - Контроль программ.
     - Контроль устройств.
     - Веб-Контроль.
     - Адаптивный контроль аномалий.
   - Отчет о шифровании данных. Содержит информации о выполненных задачах шифрования данных.
   - Отчет задач проверки. Содержит информацию о следующих выполненных задачах проверки:
     - Полная проверка.
     - Проверка важных областей.
     - Выборочная проверка.

Информация о выполнении задачи Проверка целостности удаляется, только если установлен флажок Все отчеты.

- Отчет задач обновления. Содержит информацию о выполненных задачах обновления.
- Отчет компонента Сетевой экран. Содержит информацию о работе Сетевого экрана.
- Отчет компонента Endpoint Sensor. Содержит информацию о работе компонента Endpoint Sensor.

5. Нажмите на кнопку OK.

Самозащита Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обеспечивает безопасность компьютера от вредоносных программ, включая и вредоносные программы, которые пытаются заблокировать работу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready или удалить программу с компьютера.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обеспечивает стабильность системы безопасности компьютера за счет следующих технологий:

- Механизм самозащита. Предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.
- AM-PPL (Antimalware Protected Process Light). Защищает процессы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready от вредоносных действий. Подробнее о технологии AM-PPL см. на сайте Microsoft.

Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.

- Механизм защиты от внешнего управления. Позволяет блокировать все попытки управления службами программы с удаленного компьютера.

Под управлением 64-разрядных операционных систем доступно только управление механизмом самозащиты Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready от изменения или удаления файлов программы на жестком диске, а также от изменения или удаления записей в системном реестре.

Включение и выключение механизма самозащиты

По умолчанию механизм самозащиты Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready включен.

Чтобы включить или выключить механизм самозащиты, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Параметры программы.

3. Выполните одно из следующих действий:

   - Установите флажок Включить самозащиту, если вы хотите включить механизм самозащиты.
   - Снимите флажок Включить самозащиту, если вы хотите выключить механизм самозащиты.

4. Сохраните внесенные изменения.

Включение и выключение поддержки AM-PPL

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает технологию Antimalware Protected Process Light (далее "AM-PPL") от Microsoft. AM-PPL защищает процессы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready от вредоносных действий (например, завершение работы программы). AM-PPL разрешает запуск только доверенных процессов. Процессы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready подписаны в соответствии с требованиями безопасности Windows, поэтому являются доверенными. Подробнее о технологии AM-PPL см. на сайте Microsoft. По умолчанию технология AM-PPL включена.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready также имеет встроенные механизмы защиты процессов программы. Поддержка AM-PPL позволяет делегировать функции защиты процессов операционной системе. Таким образом, вы увеличиваете быстродействие программы и уменьшаете потребление ресурсов компьютера.

Сервис AM-PPL доступен для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.

Чтобы включить или выключить поддержку технологии AM-PPL, выполните следующие действия:

1. Выключите механизм самозащиты программы.

   Механизм самозащиты предотвращает изменение и удаление процессов программы в памяти компьютера, в том числе изменение статуса AM-PPL.

2. Запустите интерпретатор командной строки cmd от имени администратора.

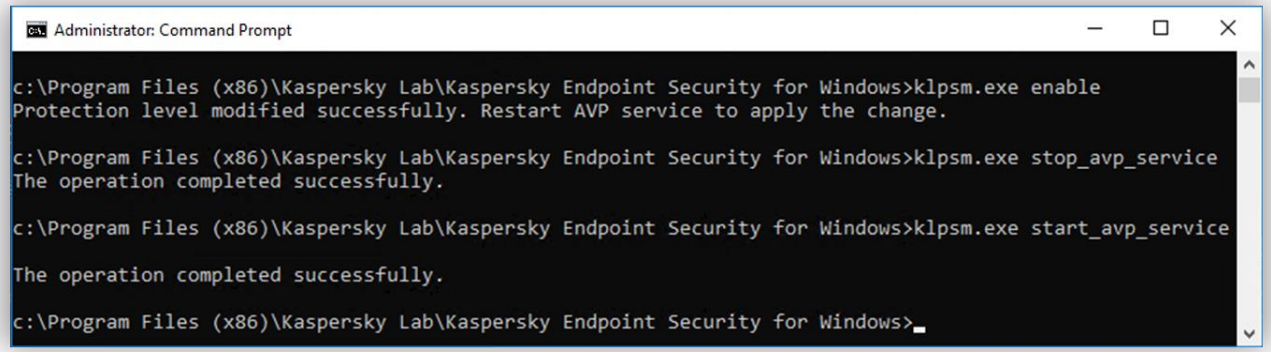
3. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

4. В командной строке введите:

   - `klpsm.exe enable` – включение поддержки технологии AM-PPL (см. рис. ниже).
   - `klpsm.exe disable` – выключение поддержки технологии AM-PPL.

5. Перезапустите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

6. Возобновите работу механизма самозащиты программы.



Включение поддержки технологии AM-PPL

Включение и выключение механизма защиты от внешнего управления

По умолчанию механизм защиты от внешнего управления включен.

Чтобы включить или выключить механизм защиты от внешнего управления, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры программы.
3. Выполните одно из следующих действий:
   - Установите флажок Выключить внешнее управление системными службами, если вы хотите включить механизм защиты от внешнего управления.
   - Снимите флажок Выключить внешнее управление системными службами, если вы хотите выключить механизм защиты от внешнего управления.

   Для завершения работы программы из командной строки необходимо, чтобы флажок Выключить внешнее управление системными службами был снят.
4. Сохраните внесенные изменения.

Обеспечение работы программ удаленного администрирования

Нередко возникают ситуации, когда при использовании механизма защиты от внешнего управления возникает необходимость применить программы удаленного администрирования.

Чтобы обеспечить работу программ удаленного администрирования, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Исключения.

3. В блоке Исключения из проверки и доверенные программы нажмите на кнопку Настройка.

   Откроется окно Доверенная зона.

4. В окне Доверенная зона выберите закладку Доверенные программы.

5. Нажмите на кнопку Добавить.

6. В раскрывшемся контекстном меню выполните одно из следующих действий:

   - Выберите пункт Программы, если вы хотите найти программу удаленного администрирования в списке установленных на компьютере программ. Откроется окно Выбор программы.

   - Выберите пункт Обзор, если вы хотите указать путь к исполняемому файлу программы удаленного администрирования.

     Откроется стандартное окно Microsoft Windows Открыть.

7. Выберите программу одним из следующих способов:

   - Если на предыдущем шаге вы выбрали пункт Программы, выберите программу в списке установленных на компьютере программ и нажмите на кнопку ОК в окне Выбор программы.

   - Если на предыдущем шаге вы выбрали пункт Обзор, укажите путь к исполняемому файлу нужной программы и нажмите на кнопку Открыть в стандартном окне Microsoft Windows Открыть.

   В результате выполненных действий откроется окно Исключения из проверки для программы.

8. Установите флажок Не контролировать активность программы.

9. Сохраните внесенные изменения.

Производительность Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и совместимость с другими программами

Производительность Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready

Под производительностью Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready подразумевается количество обнаруживаемых типов объектов, которые могут нанести вред компьютеру, а также потребление энергии и ресурсов компьютера.

Выбор типов обнаруживаемых объектов

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет гибко настраивать защиту компьютера и выбирать типы объектов, которые программа обнаруживает в ходе работы. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready всегда проверяет операционную систему на наличие вирусов, червей и троянских программ. Вы не можете выключить проверку этих типов объектов. Такие программы могут нанести значительный вред компьютеру пользователя. Чтобы обеспечить большую безопасность компьютера, вы можете расширить список обнаруживаемых типов объектов, включив контроль действий легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Использование режима энергосбережения

Во время работы на портативных компьютерах потребление программами энергоресурсов имеет особое значение. Зачастую задачи, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет по расписанию, требуют значительного количества ресурсов. При питании компьютера от аккумулятора для экономии его заряда вы можете использовать режим энергосбережения.

Режим энергосбережения позволяет автоматически откладывать выполнение задач, для которых

установлен запуск по расписанию: задача обновления; задача полной проверки; задача проверки важных

- областей; задача выборочной проверки; задача проверки целостности.
- Независимо от того, включен режим энергосбережения или нет, Kaspersky Endpoint Security для
- бизнеса - Расширенный EDR Ready
приостанавливает выполнение задач шифрования при переходе портативного компьютера в режим
- работы от аккумулятора. При выходе портативного компьютера из режима работы от аккумулятора в режим работы от сети программа возобновляет выполнение задач шифрования.
-

Передача ресурсов компьютера другим программам

Потребление ресурсов компьютера Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может сказываться на производительности других программ. Чтобы решить проблему совместной работы при увеличении нагрузки на процессор и дисковые подсистемы, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может приостанавливать выполнение задач по расписанию и уступать ресурсы другим программам.

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Чтобы проверка не зависела от работы таких программ, не следует уступать им ресурсы операционной системы.

По мере необходимости вы можете запускать эти задачи вручную.

Применение технологии лечения активного заражения

Современные вредоносные программы могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. Обнаружив вредоносную активность в операционной системе, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет расширенную процедуру лечения, применяя специальную технологию лечения активного заражения. Технология лечения активного
заражения направлена на лечение операционной системы от вредоносных программ, которые уже запустили
свои процессы в оперативной памяти и мешают Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удалить их с помощью других методов. В результате угроза нейтрализуется. В процессе процедуры лечения активного заражения не рекомендуется запускать новые процессы или редактировать реестр операционной системы. Технология лечения активного заражения требует значительных ресурсов операционной системы, что может замедлить работу других программ.

После окончания процедуры лечения активного заражения на компьютере под управлением операционной системы Microsoft Windows для рабочих станций Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запрашивает у пользователя разрешение на перезагрузку компьютера. После перезагрузки компьютера Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет файлы вредоносного программного обеспечения и запускает облегченную полную проверку компьютера.

Запрос перезагрузки на компьютере под управлением операционной системы Microsoft Windows для серверов невозможен из-за особенностей программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Незапланированная перезагрузка файлового сервера может повлечь за собой проблемы, связанные с временным отказом доступа к данным файлового сервера или потерей несохраненных данных. Перезагрузку файлового сервера рекомендуется выполнять строго по расписанию. Поэтому по умолчанию технология лечения активного заражения для файловых серверов выключена.

В случае обнаружения активного заражения на файловом сервере, на Kaspersky Security Center передается событие о необходимости лечения активного заражения. Для лечения активного заражения на сервере требуется включить технологию лечения активного заражения для серверов и запустить групповую задачу Поиск вирусов в удобное для пользователей сервера время.

Выбор типов обнаруживаемых объектов

Чтобы выбрать типы обнаруживаемых объектов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Исключения.
3. В блоке Объекты для обнаружения нажмите на кнопку Настройка.

   Откроется окно Объекты для обнаружения.

4. Установите флажки для типов объектов, которые должен обнаруживать Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready:
   - Вредоносные утилиты.
   - Рекламные программы.
   - Программы автодозвона.
   - Другие.
   - Упакованные файлы, которые могут нанести вред.
   - Многократно упакованные файлы.
5. Нажмите на кнопку OK.

   Окно Объекты для обнаружения закроется. В блоке Объекты для обнаружения под надписью Включено обнаружение объектов следующих типов отобразятся выбранные вами типы объектов.
6. Сохраните внесенные изменения.

Включение и выключение технологии лечения активного заражения

Чтобы включить или выключить технологию лечения активного заражения для рабочих станций, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры программы.
3. В правой части окна выполните одно из следующих действий:
   - Установите флажок Применять технологию лечения активного заражения, если хотите включить технологию лечения активного заражения.
   - Снимите флажок Применять технологию лечения активного заражения, если хотите выключить технологию лечения активного заражения.
4. Сохраните внесенные изменения.

При запуске задачи лечения активного заражения через Kaspersky Security Center пользователю не будут доступны большинство функций операционной системы. После завершения задачи рабочая станция будет перезагружена.

Чтобы включить технологию лечения активного заражения для серверов, выполните одно из следующих действий:

- Включите технологию лечения активного заражения в свойствах активной политики Kaspersky Security Center. Для этого выполните следующие действия:

a. Откройте раздел Параметры программы окна свойств политики.

b. Установите флажок Применять технологию лечения активного заражения.

c. Нажмите на кнопку OK в окне свойств политики, чтобы сохранить внесенные изменения.

- В свойствах групповой задачи Kaspersky Security Center "Поиск вирусов" установите флажок Выполнять лечение активного заражения немедленно.

Чтобы выключить технологию лечения активного заражения для серверов, выполните одно из следующих действий:

- Выключите технологию лечения активного заражения в свойствах политики Kaspersky Security Center. Для этого выполните следующие действия:

  a. Откройте раздел Параметры программы окна свойств политики.

  b. Снимите флажок Применять технологию лечения активного заражения.

  c. Нажмите на кнопку OK в окне свойств политики, чтобы сохранить внесенные изменения.

- В свойствах групповой задачи Kaspersky Security Center "Поиск вирусов" снимите флажок Выполнять лечение активного заражения немедленно.

Включение и выключение режима энергосбережения

Чтобы включить или выключить режим энергосбережения, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры программы.
3. В блоке Производительность выполните следующие действия:

   - Установите флажок Откладывать задачи по расписанию при работе от аккумулятора, если вы хотите включить режим энергосбережения.

     Если включен режим энергосбережения, при работе от аккумулятора не запускаются следующие задачи, даже если для них задан запуск по расписанию:

     - задача обновления; задача
     - полной проверки; задача
     - проверки важных областей;
     - задача выборочной проверки;
     - задача проверки целостности.

   - Снимите флажок Откладывать задачи по расписанию при работе от аккумулятора, если вы хотите выключить режим энергосбережения. В этом случае Kaspersky Endpoint Security для

бизнеса - Расширенный EDR Ready выполняет задачи, для которых задан запуск по расписанию, независимо от источника питания компьютера.

4. Сохраните внесенные изменения.

Включение и выключение режима передачи ресурсов другим программам

Чтобы включить или выключить режим передачи ресурсов другим программам, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.

2. В окне параметров программы выберите раздел Общие параметры → Параметры программы.

3. В блоке Производительность выполните следующие действия:

- Установите флажок Уступать ресурсы другим программам, если вы хотите включить режим передачи ресурсов другим программам. При включенном режиме передачи ресурсов другим программам Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready откладывает выполнение задач, если для них задан запуск по расписанию и их выполнение замедляет работу других программ: задача обновления; задача полной проверки; задача проверки важных областей; задача выборочной проверки; задача проверки целостности.
- Снимите флажок Уступать ресурсы другим программам, если вы хотите выключить режим передачи ресурсов другим программам. В этом случае Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет задачи, для которых задан запуск по расписанию, независимо от работы других программ.

По умолчанию режим передачи ресурсов другим программам включен.

4. Сохраните внесенные изменения.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent обеспечивает взаимодействие программы с другими решениями "Лаборатории Касперского" для обнаружения сложных угроз. Подробнее о поддерживаемых решениях см. в справке Kaspersky Endpoint Agent. Решения "Лаборатории Касперского", которые поддерживает Kaspersky Endpoint Agent, зависят от версии Kaspersky Endpoint Agent.

Kaspersky Endpoint Agent входит в комплект поставки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Вы можете установить Kaspersky Endpoint Agent при установке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Для этого вам нужно выбрать компонент Endpoint Agent при установке программы (например, в инсталляционном пакете). После установки программы с компонентом Endpoint Agent в список установленных программ будут добавлены Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и Kaspersky Endpoint Agent. После удаления

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, программа Kaspersky Endpoint Agent также будет удалена автоматически.

Создание и использование конфигурационного файла

Конфигурационный файл с параметрами работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет решить следующие задачи:

- Выполнить локальную установку Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через командную строку с заранее заданными параметрами.

  Для этого требуется сохранить конфигурационный файл в той же папке, где находится дистрибутив.

- Выполнить удаленную установку Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через Kaspersky Security Center с заранее заданными параметрами.

- Перенести параметры работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с одного компьютера на другой.

Чтобы создать конфигурационный файл, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Управление параметрами.
3. В блоке Управление параметрами нажмите на кнопку Сохранить.

   Откроется стандартное окно Microsoft Windows Выбор конфигурационного файла.
4. Укажите путь, по которому вы хотите сохранить конфигурационный файл, и введите его имя.

   Чтобы использовать конфигурационный файл для локальной или удаленной установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, необходимо назвать его install.cfg.
5. Нажмите на кнопку Сохранить.

Чтобы импортировать параметры работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из конфигурационного файла, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Управление параметрами.
3. В блоке Управление параметрами нажмите на кнопку Загрузить.

   Откроется стандартное окно Microsoft Windows Выбор конфигурационного файла.
4. Укажите путь к конфигурационному файлу.
5. Нажмите на кнопку Открыть.

Все значения параметров Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будут установлены в соответствии с выбранным конфигурационным файлом.

Обмен сообщениями между пользователем и администратором

Компоненты Контроль программ, Контроль устройств, Веб-Контроль и Адаптивный контроль аномалий предоставляют пользователям локальной сети организации, на компьютерах которых установлена программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, возможность отправлять сообщения администратору.

У пользователя может возникнуть необходимость отправить сообщение администратору локальной сети организации в следующих случаях:

- Контроль устройств заблокировал доступ к устройству.

  Шаблон сообщения с запросом доступа к заблокированному устройству доступен в интерфейсе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в разделе Контроль устройств.

- Контроль программ запретил запуск программы.

  Шаблон сообщения с запросом разрешения на запуск заблокированной программы доступен в интерфейсе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в разделе Контроль программ.

- Веб-Контроль заблокировал доступ к веб-ресурсу.

  Шаблон сообщения с запросом доступа к заблокированному веб-ресурсу доступен в интерфейсе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в разделе Веб-Контроль.

Способ отправки сообщений, а также выбор используемого шаблона зависит от наличия или отсутствия на компьютере с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready действующей политики Kaspersky Security Center и связи с Сервером администрирования Kaspersky Security Center. Возможны следующие сценарии:

- Если на компьютере с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не действует политика Kaspersky Security Center, то сообщение пользователя отправляется администратору локальной сети организации по электронной почте.

  Для заполнения полей сообщения используются значения полей из шаблона, заданного в локальном интерфейсе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.

- Если на компьютере с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready действует политика Kaspersky Security Center, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready отправляет стандартное сообщение на Сервер администрирования Kaspersky Security Center.

  В этом случае сообщения пользователей доступны для просмотра в хранилище событий Kaspersky Security Center (см. инструкцию ниже). Для заполнения полей сообщения используются значения полей из шаблона, заданного в политике Kaspersky Security Center.

- Если на компьютере с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready действует политика для автономных пользователей Kaspersky Security Center, то способ отправки сообщения зависит от наличия связи с Kaspersky Security Center:

  - Если связь с Kaspersky Security Center установлена, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready отправляет стандартное сообщение на Сервер администрирования Kaspersky Security Center.

  - Если связь с Kaspersky Security Center отсутствует, то сообщение пользователя отправляется администратору локальной сети организации по электронной почте.

Для заполнения полей сообщения в обоих случаях используются значения полей из шаблона, заданного в политике Kaspersky Security Center.

Чтобы просмотреть сообщение пользователя в хранилище событий Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В узле Сервер администрирования дерева Консоли администрирования выберите закладку События.

   В рабочей области Kaspersky Security Center отображаются все события, произошедшие во время работы программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, в том числе и сообщения администратору, приходящие от пользователей локальной сети организации.

3. Чтобы настроить фильтр событий, в раскрывающемся списке События выборки выберите элемент Запросы пользователей.

4. Выберите сообщение администратору.

5. Нажмите на кнопку Открыть окно свойств события в правой части рабочей области Консоли администрирования.

Шифрование данных

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет шифровать файлы и папки, хранящиеся на локальных дисках компьютера и съемных дисках, съемные и жесткие диски целиком. Шифрование данных снижает риски утечки информации в случае кражи / утери портативного компьютера, съемного диска или жесткого диска, а также при доступе посторонних пользователей и программ к данным. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует алгоритм шифрования Advanced Encryption Standard (AES).

Если срок действия лицензии истек, то программа не шифрует новые данные, а старые зашифрованные данные остаются зашифрованными и доступными для работы. В этом случае для шифрования новых данных требуется активировать программу по новой лицензии, которая допускает использование шифрования.

В случае истечения срока действия лицензии, нарушения Лицензионного соглашения, удаления лицензионного ключа, удаления программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready или компонентов шифрования с компьютера пользователя не гарантируется, что файлы, зашифрованные ранее, останутся зашифрованными. Это связано с тем, что некоторые программы, например Microsoft O ice Word, при редактировании файлов создают их временную копию, которой подменяют исходный файл при его сохранении. В результате при отсутствии или недоступности на компьютере функциональности шифрования файл остается незашифрованным.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обеспечивает следующие направления защиты данных:

- Шифрование файлов на локальных дисках компьютера. Вы можете сформировать списки из файлов по расширению или группам расширений и из папок, расположенных на локальных дисках компьютера, а также создать правила шифрования файлов, создаваемых отдельными программами. После применения политики программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует и расшифровывает следующие файлы:
  - файлы, отдельно добавленные в списки для шифрования и расшифровки; файлы,
  - хранящиеся в папках, добавленных в списки для шифрования и расшифровки;
  - файлы, создаваемые отдельными программами.
- Шифрование съемных дисков. Вы можете указать правило шифрования по умолчанию, в соответствии с которым программа выполняет одинаковое действие по отношению ко всем съемным дискам, и указать правила шифрования отдельных съемных дисков.

  Правило шифрования по умолчанию имеет меньший приоритет, чем правила шифрования, созданные для отдельных съемных дисков. Правила шифрования, созданные для съемных дисков с указанной моделью устройства, имеют меньший приоритет, чем правила шифрования, созданные для съемных дисков с указанным идентификатором устройства.

  Чтобы выбрать правило шифрования файлов на съемном диске, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет, известны ли модель устройства и его идентификатор. Далее программа выполняет одно из следующих действий:

  - Если известна только модель устройства, программа применяет правило шифрования, созданное для съемных дисков с данной моделью устройства, если такое правило есть.
  - Если известен только идентификатор устройства, программа применяет правило шифрования, созданное для съемных дисков с данным идентификатором устройства, если такое правило есть.

- Если известны и модель устройства, и идентификатор устройства, программа применяет правило шифрования, созданное для съемных дисков с данным идентификатором устройства, если такое правило есть. Если такого правила нет, но есть правило шифрования, созданное для съемных дисков с данной моделью устройства, программа применяет его. Если не заданы правила шифрования ни для данного идентификатора устройства, ни для данной модели устройства, программа применяет правило шифрования по умолчанию.

- Если неизвестны ни модель устройства, ни идентификатор устройства, программа применяет правило шифрования по умолчанию.

Программа позволяет подготовить съемный диск для работы с зашифрованными на нем файлами в портативном режиме. После включения портативного режима становится доступной работа с зашифрованными файлами на съемных дисках, подключенных к компьютеру с недоступной функциональностью шифрования.

- Управление правами доступа программ к зашифрованным файлам. Для любой программы вы можете создать правило доступа к зашифрованным файлам, запрещающее доступ к зашифрованным файлам или разрешающее доступ к зашифрованным файлам только в виде шифротекста - последовательности символов, полученной в результате применения шифрования.

- Создание зашифрованных архивов. Вы можете создавать зашифрованные архивы и защищать доступ к этим архивам паролем. Доступ к содержимому зашифрованных архивов можно получить только после ввода паролей, которыми вы защитили доступ к этим архивам. Такие архивы можно безопасно передавать по сети или на съемных дисках.

- Полнодисковое шифрование. Вы можете выбрать технологию шифрования: Шифрование диска Kaspersky или Шифрование диска BitLocker (далее также "BitLocker").

  BitLocker – технология, являющаяся частью операционной системы Windows. Если компьютер оснащен доверенным платформенным модулем (англ. Trusted Platform Module – TPM), BitLocker использует его для хранения ключей восстановления, позволяющих получить доступ к зашифрованному жесткому диску. При загрузке компьютера BitLocker запрашивает у доверенного платформенного модуля ключи восстановления жесткого диска и разблокирует его. Вы можете настроить использование пароля и / или PIN-кода для доступа к ключам восстановления.

  Вы можете указать правило полнодискового шифрования по умолчанию и сформировать список жестких дисков для исключения из шифрования. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет полнодисковое шифрование по секторам после применения политики Kaspersky Security Center. Программа шифрует сразу все логические разделы жестких дисков.

  После шифрования системных жестких дисков при последующем включении компьютера доступ к ним, а также загрузка операционной системы возможны только после прохождения процедуры аутентификации с помощью Агента аутентификации. Для этого требуется ввести пароль токена или смарт-карты, подключенных к компьютеру, или имя и пароль учетной записи Агента аутентификации, созданной системным администратором локальной сети организации с помощью задачи Управления учетными
  записями Агента аутентификации. Эти учетные записи основаны на учетных записях пользователей Microsoft Windows, под которыми пользователи выполняют вход в операционную систему. Также вы можете использовать технологию единого входа (англ. Single Sign-On – SSO), позволяющую осуществлять автоматический вход в операционную систему с помощью имени и пароля учетной записи Агента аутентификации.

Если для компьютера была создана резервная копия, затем данные компьютера были зашифрованы, после чего была восстановлена резервная копия компьютера и данные компьютера снова были зашифрованы, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready

формирует дубликаты учетных записей Агента аутентификации. Для удаления дубликатов требуется использовать утилиту klmover с ключом `dupfix`. Утилита klmover поставляется со сборкой Kaspersky Security Center. Подробнее о ее работе вы можете прочитать в справке для Kaspersky Security Center.

Доступ к зашифрованным жестким дискам возможен только с компьютеров, на которых установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с доступной функциональностью полнодискового шифрования. Это условие сводит к минимуму вероятность утечки информации, хранящейся на зашифрованном жестком диске, при использовании зашифрованного жесткого диска вне локальной сети организации.

Для шифрования жестких и съемных дисков вы можете использовать функцию Шифровать только занятое пространство. Рекомендуется применять эту функцию только для новых, ранее не использовавшихся устройств. Если вы применяете шифрование на уже используемом устройстве, рекомендуется зашифровать все устройство. Это гарантирует защиту всех данных – даже удаленных, но еще содержащих извлекаемые сведения.

Перед началом шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready получает карту секторов файловой системы. В первом потоке шифруются секторы, занятые файлами на момент запуска шифрования. Во втором потоке шифруются секторы, в которые выполнялась запись после начала шифрования. После завершения шифрования все секторы, содержащие данные, оказываются зашифрованными.

Если после завершения шифрования пользователь удаляет файл, то секторы, в которых хранился этот файл, становятся свободными для дальнейшей записи информации на уровне файловой системы, но остаются зашифрованными. Таким образом, по мере записи файлов на новом устройстве при регулярном запуске шифрования с включенной функцией Шифровать только занятое пространство на компьютере через некоторое время будут зашифрованы все секторы.

Данные, необходимые для расшифровки объектов, предоставляет Сервер администрирования Kaspersky Security Center, под управлением которого находился компьютер в момент шифрования. Если по каким-либо причинам компьютер с зашифрованными объектами попал под управление другого Сервера администрирования, то получить доступ к зашифрованным данным возможно одним из следующих способов:

- Серверы администрирования в одной иерархии:
  - Вам не нужно предпринимать никаких дополнительных действий. У пользователя останется доступ к зашифрованным объектам. Ключи шифрования распространяются на все Серверы администрирования.
- Серверы администрирования разрознены:
  - Запросить доступ к зашифрованным объектам у администратора локальной сети организации.
  - Восстановить данные на зашифрованных устройствах с помощью утилиты восстановления.
  - Восстановить конфигурацию Сервера администрирования Kaspersky Security Center, под управлением которого находился компьютер в момент шифрования, из резервной копии и использовать эту конфигурацию на Сервере администрирования, под управлением которого оказался компьютер с зашифрованными объектами.

При отсутствии доступа к зашифрованным данным следуйте специальным инструкциям по работе с зашифрованными данными (Восстановление доступа к зашифрованными файлам, Работа с зашифрованными устройствами при отсутствии доступа к ним).

Ограничения функциональности шифрования

Шифрование данных имеет следующие ограничения:

- В процессе шифрования программа создает служебные файлы. Для их хранения требуется около 0,5% нефрагментированного свободного пространства на жестком диске компьютера. Если нефрагментированного свободного пространства на жестком диске недостаточно, то шифрование не запускается до тех пор, пока не обеспечено это условие.

- Шифрование данных доступно только при использовании Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready с системой администрирования Kaspersky Security Center. Шифрование данных при использовании Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в автономном режиме невозможно, так как Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready хранит в Kaspersky Security Center ключи шифрования.

- Управление шифрованием данных доступно в Консоли администрирования Kaspersky Security Center и Kaspersky Security Center 12 Web Console. Управлять шифрованием данных в Kaspersky Security Center Cloud Console невозможно.

- Если программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready установлена на компьютере под управлением операционной системы Microsoft Windows для серверов, то доступно только полнодисковое шифрование с помощью технологии Шифрование диска BitLocker. Если программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций, то функциональность шифрования данных доступна в полном объеме.

Функциональность полнодискового шифрования с помощью технологии Шифрование диска Kaspersky недоступна для жестких дисков, которые не отвечают аппаратным и программным требованиям.

Не поддерживается совместимость между функциональностью полнодискового шифрования Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и Антивирусом Касперского для UEFI. Антивирус Касперского для UEFI запускается до загрузки операционной системы. При полнодисковом шифровании программа обнаружит отсутствие установленной операционной системы на компьютере. В результате работа Антивируса Касперского для UEFI завершится с ошибкой. Шифрование файлов (FLE) не влияет на работу Антивируса Касперского для UEFI.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не поддерживает следующие конфигурации:

- схема, при которой загрузчик расположен на одном диске, а операционная система – на другом;
- встроенное программное обеспечение стандарта UEFI 32;
-

система с технологией Intel® Rapid Start Technology и диски с разделом гибернации (hibernation partition), даже при отключенном использовании Intel® Rapid Start Technology; диски в формате MBR,

- имеющие более четырех расширенных разделов (extended partitions); система, в которой есть файл
- подкачки, расположенный не на системном диске; мультизагрузочная система с несколькими
- одновременно установленными операционными системами; динамические разделы
- (поддерживаются только разделы основного типа); диски, на которых менее 0,5% свободного
- нефрагментированного пространства; диски с размером сектора, отличным от 512 байт или 4096 байт,
- которые эмулируют 512 байт; гибридные диски.
-

Смена длины ключа шифрования (AES56 / AES256)

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует алгоритм шифрования AES (Advanced Encryption Standard).
Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает алгоритм шифрования AES с эффективной длиной ключа 256 и 56 бит. Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: Strong encryption (AES256) или Lite encryption (AES56). Библиотека шифрования AES устанавливается вместе с программой.

Смена длины ключа шифрования доступна только для Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11.2.0 и выше.

Смена длины ключа шифрования состоит из следующих этапов:

1. Расшифруйте объекты, которые программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зашифровала до начала смены длины ключа шифрования:

   a. Расшифруйте жесткие диски.

   b. Расшифруйте файлы на локальных дисках.

   c. Расшифруйте съемные диски.

   После смены длины ключа шифрования объекты, зашифрованные ранее, становятся недоступны.

2. Удалите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

3. Установите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из дистрибутива Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с другой библиотекой шифрования.

Вы также можете сменить длину ключа шифрования через обновление программы. Смена длины ключа через обновление программы доступна при выполнении следующих условий:

- На компьютере установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready версии 10 Service Pack 2 и выше.
- На компьютере не установлены компоненты шифрования данных: Шифрование файлов, Полнодисковое шифрование.

  По умолчанию компоненты шифрования данных не включены в состав Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Компонент Управление BitLocker не влияет на смену длины ключа шифрования.

Для смены длины ключа шифрования запустите файл kes_win.msi или setup_kes.exe из дистрибутива с нужной библиотекой шифрования. Также вы можете обновить программу дистанционно с помощью инсталляционного пакета.

Невозможно сменить длину ключа шифрования с помощью дистрибутива той же версии программы, которая установлена на вашем компьютере, без предварительного удаления программы.

Шифрование диска Kaspersky

Технология Шифрование диска Kaspersky доступна только для компьютеров под управлением операционной системы Windows для рабочих станций. Для компьютеров под управлением операционной системы Windows для серверов используйте технологию Шифрование диска BitLocker.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает полнодисковое шифрование в файловых системах FAT32, NTFS и exFat.

Перед запуском полнодискового шифрования программа выполняет ряд проверок на возможность шифрования устройства, в том числе и проверку совместимости системного жесткого диска с Агентом аутентификации или с компонентами шифрования BitLocker. Для проверки совместимости требуется выполнить перезагрузку компьютера. После перезагрузки компьютера программа в автоматическом режиме выполняет все необходимые проверки. Если проверка на совместимость проходит успешно, то после загрузки операционной системы и запуска программы запускается полнодисковое шифрование. Если в процессе проверки обнаруживается несовместимость системного жесткого диска с Агентом аутентификации или с компонентами шифрования BitLocker, требуется перезагрузить компьютер с помощью аппаратной кнопки (Reset). Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready фиксирует информацию о несовместимости, на основе которой не запускает полнодисковое шифрование после старта операционной системы. В отчетах Kaspersky Security Center выводится информация об этом событии.

Если аппаратная конфигурация компьютера изменилась, то для проверки системного жесткого диска на совместимость с Агентом аутентификации и компонентами шифрования BitLocker требуется удалить информацию о несовместимости, полученную программой при предыдущей проверке. Для этого перед полнодисковым шифрованием в командной строке требуется ввести команду `avp pbatestreset`. Если после проверки системного жесткого диска на совместимость с Агентом аутентификации операционная система не может запуститься, требуется удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации, с помощью утилиты восстановления, далее запустить Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и выполнить команду `avp pbatestreset` повторно.

После запуска полнодисковое шифрование Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует все, что записывается на жесткие диски.

Если во время полнодискового шифрования пользователь выключает или перезагружает компьютер, то перед последующей загрузкой операционной системы загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready возобновляет полнодисковое шифрование.

Если во время полнодискового шифрования операционная система переходит в режим гибернации (hibernation mode), то при выводе операционной системы из режима гибернации загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready возобновляет полнодисковое шифрование.

Если во время полнодискового шифрования операционная система переходит в спящий режим (sleep mode), то при выводе операционной системы из спящего режима Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready возобновляет полнодисковое шифрование без загрузки Агента аутентификации.

Аутентификация пользователя в Агенте аутентификации может выполняться двумя способами:

- путем ввода имени и пароля учетной записи Агента аутентификации, созданной администратором локальной сети организации средствами Kaspersky Security Center;
- путем ввода пароля подключенного к компьютеру токена или смарт-карты.

> Использование токена или смарт-карты доступно, только если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES256. Если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES56, то в добавлении файла электронного сертификата в команду будет отказано.

Агент аутентификации поддерживает раскладки клавиатуры для следующих языков:

- Английский (Великобритания);
- Английский (США);

- Арабский (Алжир, Марокко, Тунис, раскладка AZERTY);
- Испанский (Латинская Америка);
- Итальянский;
- Немецкий (Германия и Австрия);
- Немецкий (Швейцария);
- Португальский (Бразилия, раскладка ABNT2);
- Русский (для 105-клавишных клавиатур IBM / Windows с раскладкой ЙЦУКЕН);
- Турецкий (раскладка QWERTY);
- Французский (Франция);
- Французский (Швейцария);
- Французский (Бельгия, раскладка AZERTY);
- Японский (для 106-клавишных клавиатур с раскладкой QWERTY).

Раскладка клавиатуры становится доступной в Агенте аутентификации, если она добавлена в настройках языка и региональных стандартов операционной системы и доступна на экране приветствия Microsoft Windows.

Если имя учетной записи Агента аутентификации содержит символы, которые невозможно ввести с помощью доступных в Агенте аутентификации раскладок клавиатуры, то доступ к зашифрованным жестким дискам возможен только после их восстановления с помощью утилиты восстановления или после восстановления имени и пароля учетной записи Агента аутентификации.

Полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky

Перед запуском полнодискового шифрования рекомендуется убедиться в том, что компьютер не заражен. Для этого запустите полную проверку или проверку важных областей компьютера. Выполнение полнодискового шифрования на компьютере, зараженном руткитом, может привести к неработоспособности компьютера.

Чтобы выполнить полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку Политики.

4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

5. В окне политики выберите Шифрование данных → Полнодисковое шифрование.

6. В раскрывающемся списке Технология шифрования выберите элемент Шифрование диска Kaspersky.

Применение технологии шифрования Шифрование диска Kaspersky невозможно, если на компьютере есть жесткие диски, зашифрованные с помощью BitLocker.

7. В раскрывающемся списке Режим шифрования выберите действие Шифровать все жесткие диски.

Если на компьютере установлено несколько операционных систем, то после шифрования всех жестких дисков вы сможете выполнить загрузку только той операционной системы, в которой установлена программа.

Если некоторые жесткие диски нужно исключить из шифрования, сформируйте их список.

8. Выберите один из следующих способов шифрования:

- Если вы хотите применить шифрование только к тем секторам жесткого диска, которые заняты файлами, установите флажок Шифровать только занятое пространство.

  Если вы применяете шифрование на уже используемом диске, рекомендуется зашифровать весь диск.

  Это гарантирует защиту всех данных – даже удаленных, но еще содержащих извлекаемые сведения. Функцию Шифровать только занятое пространство рекомендуется использовать для новых, ранее не использовавшихся дисков.

- Если вы хотите применить шифрование ко всему жесткому диску, снимите флажок Шифровать только занятое пространство.

Если устройство было зашифровано ранее с использованием функции Шифровать только занятое пространство, после применения политики в режиме Шифровать все жесткие диски секторы, не занятые файлами, по-прежнему не будут зашифрованы.

9. Если в ходе шифрования компьютера возникла проблема несовместимости с аппаратным обеспечением, вы можете установить флажок Использовать Legacy USB Support.

Legacy USB Support – функция BIOS / UEFI, которая позволяет использовать USB-устройства (например, токен) на этапе загрузки компьютера до запуска операционной системы (BIOS-режим). Функция Legacy USB Support не влияет на поддержку USB-устройств после запуска операционной системы.

При включенной функции Legacy USB Support Агент аутентификации в BIOS-режиме не поддерживает работу с токенами по USB. Функцию рекомендуется использовать только при возникновении проблемы несовместимости с аппаратным обеспечением и только для тех компьютеров, на которых возникла проблема.

10. Сохраните внесенные изменения.

Если системные жесткие диски зашифрованы, перед загрузкой операционной системы загружается Агент аутентификации. С помощью Агента аутентификации требуется пройти процедуру аутентификации для получения доступа к зашифрованным системным жестким дискам и загрузки операционной системы. После успешного прохождения процедуры аутентификации загружается операционная система. При последующих перезагрузках операционной системы требуется повторно проходить процедуру аутентификации.

Формирование списка жестких дисков для исключения из шифрования

Вы можете сформировать список исключений из шифрования только для технологии Шифрование диска Kaspersky.

Чтобы сформировать список жестких дисков для исключения из шифрования, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Полнодисковое шифрование.
6. В раскрывающемся списке Технология шифрования выберите вариант Шифрование диска Kaspersky.

   В таблице Не шифровать следующие жесткие диски отобразятся записи о жестких дисках, которые программа не будет шифровать. Если вы ранее не сформировали список жестких дисков для исключения из шифрования, эта таблица пуста.
7. Если вы хотите добавить жесткие диски в список жестких дисков, которые программа не будет шифровать, выполните следующие действия:

   a. Нажмите на кнопку Добавить.

      Откроется окно Добавление устройств из списка Kaspersky Security Center.

   b. В окне Добавление устройств из списка Kaspersky Security Center укажите значения параметров Название, Компьютер, Тип диска, Шифрование диска Kaspersky.

   c. Нажмите на кнопку Обновить.

   d. В графе Название установите флажки в строках таблицы, соответствующих тем жестким дискам, которые вы хотите добавить в список жестких дисков для исключения из шифрования. e. Нажмите на кнопку OK.

Выбранные жесткие диски отобразятся в таблице Не шифровать следующие жесткие диски.

8. Если вы хотите удалить жесткие диски из таблицы исключений, выберите одну или несколько строк в таблице Не шифровать следующие жесткие диски и нажмите на кнопку Удалить.

   Чтобы выбрать несколько строк в таблице, выделяйте их, удерживая клавишу CTRL.

9. Сохраните внесенные изменения.

Включение использования технологии единого входа (SSO)

Технология единого входа (англ. Single Sign-On – SSO) позволяет выполнить автоматический вход в операционную систему с помощью учетных данных Агента аутентификации.

При использовании технологии единого входа Агент аутентификации игнорирует требования к надежности пароля, заданные в Kaspersky Security Center. Вы можете задать требования к надежности пароля в параметрах операционной системы.

Технология единого входа несовместима со сторонними поставщиками учетных данных.

Как включить использование технологии единого входа в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Общие параметры шифрования.
6. В блоке Параметры паролей нажмите на кнопку Настройка.
7. В открывшемся окне на закладке Агент аутентификации установите флажок Использовать технологию единого входа (SSO).
8. Сохраните внесенные изменения.

В результате пользователю нужно пройти процедуру аутентификации только один раз с помощью агента. Проходить процедуру аутентификации для загрузки операционной системы не требуется. Операционная система загружается автоматически.

Как включить использование технологии единого входа в Web Console

1. В главном окне Web Console выберите закладку Устройства → Политики и профили политик.
2. Нажмите на название политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для компьютеров, на которых вы хотите включить использование технологии единого входа.

Откроется окно свойств политики.

3. Выберите закладку Параметры программы.

4. Перейдите в раздел Шифрование данных → Полнодисковое шифрование.

5. Выберите технологию Шифрование диска Kaspersky и перейдите по ссылке для настройки параметров.

Откроются параметры шифрования.

6. В блоке Параметры паролей установите флажок Использовать технологию единого входа (SSO).

7. Нажмите на кнопку OK.

В результате пользователю нужно пройти процедуру аутентификации только один раз с помощью агента. Проходить процедуру аутентификации для загрузки операционной системы не требуется. Операционная система загружается автоматически.

Для работы технологии единого входа пароль учетной записи Windows и пароль учетной записи Агента аутентификации должны совпадать. Если пароли не совпадают, то пользователю нужно выполнить процедуру аутентификации дважды: в интерфейсе Агента аутентификации и перед загрузкой операционной системы. После этого Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заменит пароль учетной записи Windows на пароль учетной записи Агента аутентификации.

Управление учетными записями Агента аутентификации

Агент аутентификации нужен для работы с дисками, которые защищены с помощью технологии Шифрование диска Kaspersky (FDE). Перед загрузкой операционной системы пользователю нужно пройти аутентификацию с помощью агента. Для настройки параметров аутентификации пользователей предназначена задача Управление учетными записями Агента аутентификации. Вы можете использовать как локальные задачи для отдельных компьютеров, так и групповые задачи для компьютеров из отдельных групп администрирования или выборки компьютеров.

Настроить расписание запуска задачи Управление учетными записями Агента аутентификации невозможно. Также невозможно принудительно остановить выполнение задачи.

Как создать задачу Управление учетными записями Агента аутентификации в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку Сервер администрирования → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Новая задача.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0) → Управление учетными записями Агента аутентификации.

Шаг 2. Выбор команды управления учетными записями Агента аутентификации

Сформируйте список команд управления учетными записями Агента аутентификации. Команды управления позволяют добавлять, изменять и удалять учетные записи Агента аутентификации (см. инструкции ниже). Только пользователи, которые имеют учетную запись Агента аутентификации, могут пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Определение названия задачи

Введите название задачи, например, `Учетные записи администраторов`.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок Запустить задачу после завершения работы мастера. Вы можете следить за ходом выполнения задачи в свойствах задачи.

В результате после выполнения задачи при следующей загрузке компьютера новый пользователь может пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Как создать задачу Управление учетными записями Агента аутентификации в Web Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на кнопку Добавить.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке Программа выберите Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Windows (11.4.0).
2. В раскрывающемся списке Тип задачи выберите Управление учетными записями Агента аутентификации.
3. В поле Название задачи введите короткое описание, например, `Учетные записи администраторов`.
4. В блоке Выбор устройств, которым будет назначена задача выберите область действия задачи.

Шаг 2. Управление учетными записями Агента аутентификации

Сформируйте список команд управления учетными записями Агента аутентификации. Команды управления позволяют добавлять, изменять и удалять учетные записи Агента аутентификации (см. инструкции ниже). Только пользователи, которые имеют учетную запись Агента аутентификации, могут пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Шаг 3. Завершение создание задачи

Завершите работу мастера по кнопке Готово. В списке задач отобразится новая задача.

Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку Запустить.

В результате после выполнения задачи при следующей загрузке компьютера новый пользователь может пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Для добавления учетной записи Агента аутентификации нужно добавить специальную команду в задачу Управление учетными записями Агента аутентификации. Групповую задачу удобно использовать, например, для добавления учетной записи администратора на все компьютеры.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready позволяет автоматически создавать учетные записи Агента аутентификации перед шифрованием диска. Вы можете включить автоматическое создание учетных записей Агента аутентификации в параметрах политики полнодискового шифрования. Также вы можете использовать технологию единого входа (SSO).

Как добавить учетную запись Агента аутентификации через Консоль администрирования (MMC)

1. Откройте свойства задачи Управление учетными записями Агента аутентификации.

2. В свойствах задачи выберите раздел Параметры.

3. Нажмите на кнопку Добавить → Команду для добавления учетной записи.

4. В открывшемся окне в поле Учетная запись Windows укажите имя учетной записи Microsoft Windows, на основе которой будет создана учетная запись Агента аутентификации.

5. Если вы ввели имя учетной записи Windows вручную, нажмите на кнопку Разрешить, чтобы определить идентификатор безопасности учетной записи (англ. SID – Security Identi er).

   Если вы не определяете идентификатор безопасности по кнопке Разрешить, то он будет определен в момент выполнения задачи на компьютере.

   > Определение идентификатора безопасности учетной записи Windows нужно для проверки корректности ввода имени учетной записи Windows. Если учетная запись Windows не существует на компьютере или в доверенном домене, задача Управление учетными записями Агента аутентификации будет завершена с ошибкой.

6. Установите флажок Заменить существующую учетную запись, если вы хотите, чтобы уже заведенная для Агента аутентификации учетная запись с таким же именем была заменена на добавляемую.

   > Этот шаг доступен, если вы добавляете команду для создания учетной записи Агента аутентификации в свойствах групповой задачи управления учетными записями Агента аутентификации. Этот шаг недоступен, если вы добавляете команду для создания учетной записи Агента аутентификации в свойствах локальной задачи Шифрование всего носителя, управление учетными записями.

7. В поле Имя пользователя введите имя учетной записи Агента аутентификации, которое требуется вводить при аутентификации для доступа к зашифрованным жестким дискам.

8. Установите флажок Разрешать вход по паролю, если вы хотите, чтобы при аутентификации для получения доступа к зашифрованным жестким дискам программа требовала пароль учетной записи Агента аутентификации. Задайте пароль учетной записи Агента аутентификации. Если нужно, вы можете запросить у пользователя новый пароль после первой аутентификации.

9. Установите флажок Разрешать вход по сертификату, если вы хотите, чтобы при аутентификации для доступа к зашифрованным жестким дискам программа требовала подключения токена или смарткарты к компьютеру. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена.

10. Если требуется, в поле Описание команды введите информацию об учетной записи Агента аутентификации, необходимую вам для работы с командой.

11. Выполните одно из следующих действий:

    - Выберите вариант Разрешать аутентификацию, если вы хотите, чтобы программа разрешала доступ к аутентификации в Агенте аутентификации пользователю, работающему под учетной записью, указанной в команде.

- Выберите вариант Запрещать аутентификацию, если вы хотите, чтобы программа запрещала доступ к аутентификации в Агенте аутентификации пользователю, работающему под учетной записью, указанной в команде.

12. Сохраните внесенные изменения.

Как добавить учетную запись Агента аутентификации через Web Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready Управление учетными записями Агента аутентификации.

   Откроется окно свойств задачи.

3. Выберите закладку Параметры программы.

4. В списке учетных записей Агента аутентификации нажмите на кнопку Добавить.

   Запустится мастер управления учетными записями Агента аутентификации.

5. Выберите тип команды Добавление учетной записи.

6. Выберите учетную запись пользователя. Вы можете выбрать учетную запись из списка доменных учетных записей или ввести имя учетной записи вручную. Нажмите на кнопку Далее.

   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready определяет идентификатор безопасности учетной записи (англ. SID – Security Identi er). Это нужно для проверки учетной записи. Если вы ввели имя пользователя неверно, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready завершит выполнение задачи с ошибкой.

7. Настройте параметры учетной записи Агента аутентификации:

   - Создать новую учетную запись Агента аутентификации взамен существующей. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет существующие учетные записи на компьютере. Если идентификатор безопасности пользователя на компьютере и в задаче совпадают, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready изменит параметры учетной записи в в соответствии с задачей.

   - Имя пользователя. По умолчанию имя пользователя учетной записи Агента аутентификации соответствует доменному имени пользователя.

   - Разрешить вход по паролю. Задайте пароль учетной записи Агента аутентификации. Если нужно, вы можете запросить у пользователя новый пароль после первой аутентификации. Таким образом, у каждого пользователя будет свой уникальный пароль. Также вы можете задать требования к надежности пароля для учетной записи Агента аутентификации в политике.

   - Разрешить вход по сертификату. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена. Таким образом, пользователю нужно будет ввести пароль от смарткарты или токена.

   - Доступ учетной записи к зашифрованным данным. Настройте доступ пользователя к зашифрованному диску. Вы можете, например, временно запретить аутентификацию пользователя и не удалять учетную запись Агента аутентификации.

   - Комментарий. Введите описание учетной записи, если требуется.

8. Сохраните внесенные изменения.

9. Установите флажок напротив задачи и нажмите на кнопку Запустить.

В результате после выполнения задачи при следующей загрузке компьютера новый пользователь может пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Для изменения пароля и других данных учетной записи Агента аутентификации нужно добавить специальную команду в задачу Управление учетными записями Агента аутентификации. Групповую задачу удобно использовать, например, для замены сертификата токена администратора на всех компьютерах.

Как изменить учетную запись Агента аутентификации через Консоль администрирования (MMC)

1. Откройте свойства задачи Управление учетными записями Агента аутентификации.
2. В свойствах задачи выберите раздел Параметры.
3. Нажмите на кнопку Добавить → Команду для изменения учетной записи.
4. В открывшемся окне в поле Учетная запись Windows укажите имя учетной записи пользователя Microsoft Windows, которую вы хотите изменить.
5. Если вы ввели имя учетной записи Windows вручную, нажмите на кнопку Разрешить, чтобы определить идентификатор безопасности учетной записи (англ. SID – Security Identi er).

   Если вы не определяете идентификатор безопасности по кнопке Разрешить, то он будет определен в момент выполнения задачи на компьютере.

   > Определение идентификатора безопасности учетной записи Windows нужно для проверки корректности ввода имени учетной записи Windows. Если учетная запись Windows не существует на компьютере или в доверенном домене, задача Управление учетными записями Агента аутентификации будет завершена с ошибкой.

6. Установите флажок Изменить имя пользователя и введите новое имя учетной записи Агента аутентификации, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле Учетная запись Windows, программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready изменила имя пользователя на указанное в поле ниже.
7. Установите флажок Изменить параметры входа по паролю, если вы хотите сделать доступными для изменения параметры входа по паролю.
8. Установите флажок Разрешать вход по паролю, если вы хотите, чтобы при аутентификации для получения доступа к зашифрованным жестким дискам программа требовала пароль учетной записи Агента аутентификации. Задайте пароль учетной записи Агента аутентификации.
9. Установите флажок Изменить правило смены пароля при аутентификации в Агенте аутентификации, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле Учетная запись Windows, программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready изменила значение параметра смены пароля на установленное ниже.
10. Установите значение параметра смены пароля при аутентификации в Агенте аутентификации.
11. Установите флажок Изменить параметры входа по сертификату, если вы хотите сделать доступными для изменения параметры входа по электронному сертификату токена или смарт-карте.
12. Установите флажок Разрешать вход по сертификату, если вы хотите, чтобы при аутентификации для доступа к зашифрованным жестким дискам программа требовала ввод пароля к подключенному к компьютеру токену или смарт-карте. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена.
13. Установите флажок Изменить описание команды и измените описание команды, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле Учетная запись Windows, программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready изменила описание команды.

14. Установите флажок Изменить правило доступа к аутентификации в Агенте аутентификации, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле Учетная запись Windows, программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready изменила правило доступа пользователя к аутентификации в Агенте аутентификации на установленное ниже.

15. Установите правило доступа к аутентификации в Агенте аутентификации.

16. Сохраните внесенные изменения.

Как изменить учетную запись Агента аутентификации через Web Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready Управление учетными записями Агента аутентификации.

   Откроется окно свойств задачи.

3. Выберите закладку Параметры программы.

4. В списке учетных записей Агента аутентификации нажмите на кнопку Добавить.

   Запустится мастер управления учетными записями Агента аутентификации.

5. Выберите тип команды Изменение учетной записи.

6. Выберите учетную запись пользователя. Вы можете выбрать учетную запись из списка доменных учетных записей или ввести имя учетной записи вручную. Нажмите на кнопку Далее.

   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready определяет идентификатор безопасности учетной записи (англ. SID – Security Identi er). Это нужно для проверки учетной записи. Если вы ввели имя пользователя неверно, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready завершит выполнение задачи с ошибкой.

7. Установите флажки напротив тех параметров, которые вы хотите изменить.

8. Настройте параметры учетной записи Агента аутентификации:

   - Создать новую учетную запись Агента аутентификации взамен существующей. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет существующие учетные записи на компьютере. Если идентификатор безопасности пользователя на компьютере и в задаче совпадают, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready изменит параметры учетной записи в в соответствии с задачей.

   - Имя пользователя. По умолчанию имя пользователя учетной записи Агента аутентификации соответствует доменному имени пользователя.

   - Разрешить вход по паролю. Задайте пароль учетной записи Агента аутентификации. Если нужно, вы можете запросить у пользователя новый пароль после первой аутентификации. Таким образом, у каждого пользователя будет свой уникальный пароль. Также вы можете задать требования к надежности пароля для учетной записи Агента аутентификации в политике.

   - Разрешить вход по сертификату. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена. Таким образом, пользователю нужно будет ввести пароль от смарткарты или токена.

   - Доступ учетной записи к зашифрованным данным. Настройте доступ пользователя к зашифрованному диску. Вы можете, например, временно запретить аутентификацию пользователя и не удалять учетную запись Агента аутентификации.

   - Комментарий. Введите описание учетной записи, если требуется.

9. Сохраните внесенные изменения.

10. Установите флажок напротив задачи и нажмите на кнопку Запустить.

Для удаления учетной записи Агента аутентификации нужно добавить специальную команду в задачу Управление учетными записями Агента аутентификации. Групповую задачу удобно использовать, например, для удаления учетной записи уволенного сотрудника.

Как удалить учетную запись Агента аутентификации через Консоль администрирования (MMC)

1. Откройте свойства задачи Управление учетными записями Агента аутентификации.
2. В свойствах задачи выберите раздел Параметры.
3. Нажмите на кнопку Добавить → Команду для удаления учетной записи.
4. В открывшемся окне в поле Учетная запись Windows укажите имя учетной записи пользователя Windows, на основе которой создана учетная запись для Агента аутентификации, которую вы хотите удалить.
5. Если вы ввели имя учетной записи Windows вручную, нажмите на кнопку Разрешить, чтобы определить идентификатор безопасности учетной записи (англ. SID – Security Identi er).

   Если вы не определяете идентификатор безопасности по кнопке Разрешить, то он будет определен в момент выполнения задачи на компьютере.

   Определение идентификатора безопасности учетной записи Windows нужно для проверки корректности ввода имени учетной записи Windows. Если учетная запись Windows не существует на компьютере или в доверенном домене, задача Управление учетными записями Агента аутентификации будет завершена с ошибкой.
6. Сохраните внесенные изменения.

Как удалить учетную запись Агента аутентификации через Web Console

1. В главном окне Web Console выберите Устройства → Задачи.

   Откроется список задач.
2. Нажмите на задачу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready Управление учетными записями Агента аутентификации.

   Откроется окно свойств задачи.
3. Выберите закладку Параметры программы.
4. В списке учетных записей Агента аутентификации нажмите на кнопку Добавить.

   Запустится мастер управления учетными записями Агента аутентификации.
5. Выберите тип команды Удаление учетной записи.
6. Выберите учетную запись пользователя. Вы можете выбрать учетную запись из списка доменных учетных записей или ввести имя учетной записи вручную.
7. Сохраните внесенные изменения.
8. Установите флажок напротив задачи и нажмите на кнопку Запустить.

В результате после выполнения задачи при следующей загрузке компьютера пользователь не сможет пройти процедуру аутентификацию и загрузить операционную систему. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запретит доступ к зашифрованным данным.

Для просмотра списка пользователей, которые могут пройти аутентификацию с помощью агента и загрузить операционную систему, нужно перейти в свойства управляемого компьютера.

Как просмотреть список учетных записей Агента аутентификации через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Устройства.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел Задачи.

   Откроется список локальных задач.
6. Выберите задачу Управление учетными записями Агента аутентификации.
7. В свойствах задачи выберите раздел Параметры.

В результате вам будет доступен список учетных записей Агента аутентификации на этом компьютере. Только пользователи из списка могут пройти аутентификацию с помощью агента и загрузить операционную систему.

Как просмотреть список учетных записей Агента аутентификации через Web Console

1. В главном окне Web Console выберите Устройства → Управляемые устройства.
2. Нажмите на имя компьютера, на котором вы хотите просмотреть список учетных записей Агента аутентификации.

   Откроются свойства компьютера.
3. В окне свойств компьютера выберите раздел Задачи.

   Откроется список локальных задач.
4. Выберите задачу Управление учетными записями Агента аутентификации.
5. В свойствах задачи выберите закладку Параметры программы.

В результате вам будет доступен список учетных записей Агента аутентификации на этом компьютере. Только пользователи из списка могут пройти аутентификацию с помощью агента и загрузить операционную систему.

Использование токена и смарт-карты при работе с Агентом аутентификации

При аутентификации для доступа к зашифрованным жестким дискам можно использовать токен или смарткарту. Для этого необходимо добавить файл электронного сертификата токена или смарт-карты в задачу Управление учетными записями Агента аутентификации.

Использование токена или смарт-карты доступно, только если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES256. Если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES56, то в добавлении файла электронного сертификата в команду будет отказано.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready работает со следующими токенами, считывателями смарт-карт и смарткартами:

- SafeNet eToken PRO 64K (4.2b) (USB).
- SafeNet eToken PRO 72K Java (USB).
- SafeNet eToken PRO 72K Java (Smart Card).
- SafeNet eToken 4100 72K Java (Smart Card).
- SafeNet eToken 5100 (USB).
- SafeNet eToken 5105 (USB).
- SafeNet eToken 7300 (USB).
- EMC RSA SecurID 800 (USB).
- Рутокен ЭЦП (USB).
- Рутокен ЭЦП (Flash).
- Aladdin-RD JaCarta PKI (USB).
- Aladdin-RD JaCarta PKI (Smart Card).
- Athena IDProtect Laser (USB).
- Gemalto IDBridge CT40 (Reader).
- Gemalto IDPrime .NET 511.

Чтобы добавить файл электронного сертификата токена или смарт-карты в команду для создания учетной записи Агента аутентификации, его требуется предварительно сохранить с помощью стороннего программного обеспечения, предназначенного для управления сертификатами.

Сертификат токена или смарт-карты должен обладать следующими свойствами:

- Сертификат удовлетворяет стандарту X.509, а файл сертификата имеет кодировку DER.
- Сертификат содержит RSA-ключ длиной не менее 1024 бит.

Если электронный сертификат токена или смарт-карты не удовлетворяет этим требованиям, загрузить файл сертификата в команду для создания учетной записи Агента аутентификации невозможно.

Также параметр `KeyUsage` сертификата должен иметь значение `keyEncipherment` или `dataEncipherment`. Параметр `KeyUsage` определяет назначение сертификата. Если параметр имеет другое значение, Kaspersky Security Center загрузит файл сертификата, но покажет предупреждение.

Если пользователь потерял токен или смарт-карту, администратору требуется добавить файл электронного сертификата нового токена или новой смарт-карты в команду для создания учетной записи Агента аутентификации. После этого пользователю требуется пройти процедуру получения доступа к зашифрованным устройствам или восстановления данных на зашифрованных устройствах.

Расшифровка жестких дисков

Вы можете расшифровать жесткие диски даже при отсутствии действующей лицензии, допускающей шифрование данных.

Чтобы расшифровать жесткие диски, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Полнодисковое шифрование.
6. В раскрывающемся списке Технология шифрования выберите ту технологию, с помощью которой были зашифрованы жесткие диски.
7. Выполните одно из следующих действий:
   - В раскрывающемся списке Режим шифрования выберите элемент Расшифровывать все жесткие диски, если вы хотите расшифровать все зашифрованные жесткие диски.
   - В таблицу Не шифровать следующие жесткие диски добавьте те зашифрованные жесткие диски, которые вы хотите расшифровать.

     Этот вариант доступен только для технологии шифрования Шифрование диска Kaspersky.
8. Сохраните внесенные изменения.

Если во время расшифровки жестких дисков, зашифрованных с помощью технологии Шифрование диска Kaspersky, пользователь выключает или перезагружает компьютер, то перед последующей загрузкой операционной системы загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready возобновляет расшифровку жестких дисков.

Если во время расшифровки жестких дисков, зашифрованных с помощью технологии Шифрование диска Kaspersky, операционная система переходит в режим гибернации (hibernation mode), то при выводе операционной системы из режима гибернации загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready возобновляет расшифровку жестких дисков. После расшифровки жестких дисков режим гибернации недоступен до первой перезагрузки операционной системы.

Если во время расшифровки жестких дисков операционная система переходит в спящий режим (sleep mode), то при выводе операционной системы из спящего режима Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready возобновляет расшифровку жестких дисков без загрузки Агента аутентификации.

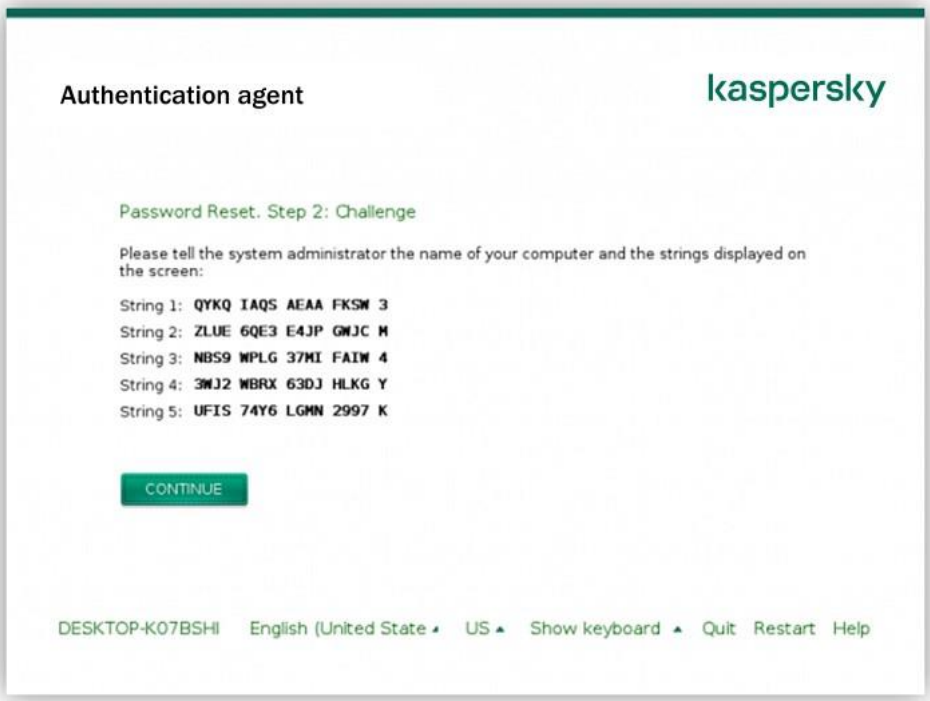
Восстановление доступа к диску, защищенному технологией Шифрование диска Kaspersky

Если пользователь забыл пароль доступа к жесткому диску, защищенному технологией Шифрование диска Kaspersky, нужно запустить процедуру восстановления ("Запрос - Ответ").

Восстановление доступа к системному жесткому диску

Восстановление доступа к системному жесткому диску, защищенному технологией Шифрование диска Kaspersky, состоит из следующих этапов:

1. Пользователь сообщает администратору блоки запроса (см. рис. ниже).
2. Администратор вводит блоки запроса в Kaspersky Security Center, получает блоки ответа и сообщает блоки ответа пользователю.
3. Пользователь вводит блоки ответа в интерфейсе Агента аутентификации и получает доступ к жесткому диску.



Восстановление доступа к системному жесткому диску, защищенного технологией Шифрование диска Kaspersky

Для запуска процедуры восстановления пользователю нужно в интерфейсе Агента аутентификации нажать на кнопку Forgot your password.

Как получить блоки ответа для системного жесткого диска, защищенного технологией Шифрование диска Kaspersky, в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Устройства.
4. На закладке Устройства выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт Предоставление доступа в офлайн-режиме.
6. В открывшемся окне выберите закладку Агент аутентификации.
7. В блоке Используемый алгоритм шифрования выберите алгоритм шифрования: AES56 или AES256.

   Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: Strong encryption (AES256) или Lite encryption (AES56). Библиотека шифрования AES устанавливается вместе с программой.
8. В раскрывающемся списке Учетная запись выберите имя учетной записи Агента аутентификации пользователя, запросившего восстановление доступа к диску.
9. В раскрывающемся списке Жесткий диск выберите зашифрованный жесткий диск, доступ к которому необходимо восстановить.
10. В блоке Запрос пользователя введите блоки запроса, продиктованные пользователем.

    В результате содержимое блоков ответа на запрос пользователя о восстановлении имени и пароля учетной записи Агента аутентификации отобразится в поле Ключ доступа. Передайте содержимое блоков ответа пользователю.

Как получить блоки ответа для системного жесткого диска, защищенного технологией Шифрование диска Kaspersky, в Web Console

1. В главном окне Web Console выберите Устройства → Управляемые устройства.
2. Установите флажок рядом с именем компьютера, доступ к диску которого вы хотите восстановить.
3. Нажмите на кнопку Предоставить доступ к устройству в автономном режиме.
4. В открывшемся окне выберите раздел Агент аутентификации.
5. В раскрывающемся списке Учетная запись выберите имя учетной записи Агента аутентификации, созданной для пользователя, запросившего восстановление имени и пароля учетной записи Агента аутентификации.
6. Введите блоки запроса, продиктованные пользователем.

   Содержимое блоков ответа на запрос пользователя о восстановлении имени и пароля учетной записи

Агента аутентификации отобразится внизу окна. Передайте содержимое блоков ответа пользователю.

После прохождения процедуры восстановления Агент аутентификации предложит пользователю сменить пароль.

Восстановление доступа к несистемному жесткому диску

Восстановление доступа к несистемному жесткому диску, защищенному технологией Шифрование диска Kaspersky, состоит из следующих этапов:

1. Пользователь отправляет администратору файл запроса.
2. Администратор добавляет файл запроса в Kaspersky Security Center, создает файл ключа доступа и отправляет файл пользователю.
3. Пользователь добавляет файл ключа доступа в Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и получает доступ к жесткому диску.

Для запуска процедуры восстановления пользователю нужно обратиться к жесткому диску. В результате Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создаст файл запроса (файл с расширением kesdc), который пользователю нужно передать администратору, например, по электронной почте.

Как получить файл ключа доступа к зашифрованному несистемному жесткому диску в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Устройства.
4. На закладке Устройства выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт Предоставление доступа в офлайн-режиме.
6. В открывшемся окне выберите закладку Шифрование данных.
7. На закладке Шифрование данных нажмите на кнопку Обзор.
8. В окне выбора файла запроса укажите путь к файлу, полученного от пользователя.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.

Как получить файл ключа доступа к зашифрованному несистемному жесткому диску в Web Console

1. В главном окне Web Console выберите Устройства → Управляемые устройства.

2. Установите флажок рядом с именем компьютера, доступ к данным которого вы хотите восстановить.

3. Нажмите на кнопку Предоставить доступ к устройству в автономном режиме.

4. Выберите раздел Шифрование данных.

5. Нажмите на кнопку Выбрать файл и выберите файл запроса, полученный от пользователя (файл с расширением kesdc).

Web Console покажет информацию о запросе. В том числе, имя компьютера, на котором пользователь запрашивает доступ к файлу.

6. Нажмите на кнопку Сохранить ключ и выберите папку для сохранения файла ключа доступа к зашифрованным данным (файл с расширением kesdr).

В результате вам будет доступен ключ доступа к зашифрованным данным, который нужно будет передать пользователю.

Обновление операционной системы

Обновление операционной системы компьютера, защищенного с помощью полнодискового шифрования (FDE), имеет ряд особенностей. Выполняйте обновление операционной системы последовательно: сначала обновите ОС на одном компьютере, затем на небольшой части компьютеров, затем на всех компьютерах сети.

Если вы используете технологию Шифрование диска Kaspersky, то перед запуском операционной системы загружается Агент аутентификации. С помощью Агента аутентификации пользователь выполняет вход в систему и получает доступ к зашифрованным дискам. Далее начинается загрузка операционной системы.

Если запустить обновление операционной системы на компьютере, защищенном с помощью технологии Шифрование диска Kaspersky, мастер обновления ОС может удалить Агент аутентификации. В результате компьютер может быть заблокирован, так как загрузчик ОС не сможет получить доступ к зашифрованному диску.

Подробнее о безопасном обновлении операционной системы вы можете узнать в базе знаний Службы технической поддержки.

Автоматическое обновление операционной системы доступно при выполнении следующих условий:

1. Обновление ОС через WSUS (Windows Server Update Services).

2. На компьютере установлена операционная система Windows 10 версия 1607 (RS1) и выше.

3. На компьютере установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready версии 11.2.0 и выше.

При выполнении всех условий вы можете обновлять операционную систему обычным способом.

Если вы используете технологию Шифрование диска BitLocker, для обновления Windows 10 не нужно расшифровывать жесткие диски. Подробнее о BitLocker см. на сайте Microsoft.

Устранение ошибок при обновлении функциональности шифрования

При обновлении с предыдущих версий программы до Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready для Windows 11.4.0 обновляется функциональность полнодискового шифрования.

При запуске обновления функциональности полнодискового шифрования могут возникнуть следующие ошибки:

- Не удалось инициализировать обновление.
- Устройство несовместимо с Агентом аутентификации.

Чтобы устранить ошибки, возникшие при запуске обновления функциональности полнодискового шифрования, в новой версии программы выполните следующие действия:

1. Расшифруйте жесткие диски.
2. Повторно зашифруйте жесткие диски.

В процессе обновления функциональности полнодискового шифрования могут возникнуть следующие ошибки:

- Не удалось завершить обновление.
- Откат обновления функциональности шифрования завершен с ошибкой.

Чтобы устранить ошибки, возникшие в процессе обновления функциональности полнодискового шифрования, восстановите доступ к зашифрованному устройству с помощью утилиты восстановления.

Выбор уровня трассировки Агента аутентификации

Программа записывает служебную информацию о работе Агента аутентификации, а также информацию о действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.

Чтобы выбрать уровень трассировки Агента аутентификации, выполните следующие действия:

1. Сразу после запуска компьютера с зашифрованными жесткими дисками по кнопке F3 вызовите окно для настройки параметров Агента аутентификации.
2. В окне настройки параметров Агента аутентификации выберите уровень трассировки:
   - Disable debug logging (default). Если выбран этот вариант, то программа не записывает информацию о событиях работы Агента аутентификации в файл трассировки.
   - Enable debug logging. Если выбран этот вариант, то программа записывает информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.
   - Enable verbose logging. Если выбран этот вариант, то программа записывает детальную информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте

аутентификации, в файл трассировки.

Уровень детализации записей для этого варианта выше, чем при выборе уровня Enable debug logging. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

- Enable debug logging and select serial port. Если выбран этот вариант, то программа записывает информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки, а также передает ее через COM-порт.

  Если компьютер с зашифрованными жесткими дисками соединен с другим компьютером через COMпорт, то события работы Агента аутентификации можно исследовать с помощью этого компьютера.

- Enable verbose debug logging and select serial port. Если выбран этот вариант, то программа записывает детальную информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки, а также передает ее через COM-порт.

Уровень детализации записей для этого варианта выше, чем при выборе уровня Enable debug logging and select serial port. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

Запись в файл трассировки Агента аутентификации выполняется в случае, если на компьютере есть зашифрованные жесткие диски или выполняется полнодисковое шифрование.

Файл трассировки Агента аутентификации не передается в "Лабораторию Касперского", как другие файлы трассировки программы. При необходимости вы можете самостоятельно отправить файл трассировки Агента аутентификации в "Лабораторию Касперского" для анализа.

Изменение справочных текстов Агента аутентификации

Перед изменением справочных текстов Агента аутентификации ознакомьтесь со списком поддерживаемых символов в предзагрузочной среде (см. ниже).

Чтобы изменить справочные тексты Агента аутентификации, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Общие параметры шифрования.
6. Нажмите на кнопку Справка в блоке Шаблоны.

Откроется окно Справочные тексты Агента аутентификации.

7. Выполните следующие действия:

   - Выберите закладку Аутентификация, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе ввода учетных данных.

   - Выберите закладку Смена пароля, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе смены пароля для учетной записи Агента аутентификации.

   - Выберите закладку Восстановление пароля, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе восстановления пароля для учетной записи Агента аутентификации.

8. Измените справочные тексты.

   Если вы хотите восстановить исходный текст, нажмите на кнопку По умолчанию.

   Вы можете ввести справочный текст, содержащий 16 или менее строк. Максимальная длина строки составляет 64 символа.

9. Сохраните внесенные изменения.

Ограничения поддержки символов в справочных текстах Агента аутентификации

В предзагрузочной среде поддерживаются следующие символы Unicode:

- основная латиница (0000 - 007F); дополнительные символы Latin-1
- (0080 - 00FF); расширенная латиница-A (0100 - 017F); расширенная
- латиница-B (0180 - 024F); некомбинируемые протяженные символы-
- идентификаторы (02B0 - 02FF); комбинируемые диакритические знаки
- (0300 - 036F); греческий и коптский алфавиты (0370 - 03FF); кириллица
- (0400 - 04FF); иврит (0590 - 05FF); арабское письмо (0600 - 06FF);
- дополнительная расширенная латиница (1E00 - 1EFF); знаки пунктуации
- (2000 - 206F); символы валют (20A0 - 20CF); буквоподобные символы
- (2100 - 214F); геометрические фигуры (25A0 - 25FF); формы
- представления арабских букв-B (FE70 - FEFF).

- Символы, не указанные в этом списке, не поддерживаются в предзагрузочной среде. Не
- рекомендуется использовать такие символы в справочных текстах Агента аутентификации.

Удаление объектов и данных, оставшихся после тестовой работы Агента аутентификации

Если в процессе удаления программы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready обнаруживает объекты и данные, оставшиеся на системном жестком диске после тестовой работы Агента аутентификации, то удаление программы прерывается и становится невозможным до тех пор, пока эти объекты и данные не будут удалены.

Объекты и данные могут остаться на системном жестком диске после тестовой работы Агента аутентификации только в исключительных ситуациях. Например, если после применения политики Kaspersky Security Center с установленными параметрами шифрования компьютер не перезагружался или после тестовой работы Агента аутентификации программа не запускается.

Вы можете удалить объекты и данные, оставшиеся на системном жестком диске после тестовой работы Агента аутентификации, следующими способами: с помощью политики Kaspersky Security Center; с помощью утилиты восстановления.

Чтобы удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации, с помощью политики Kaspersky Security Center, выполните следующие действия:

1. Примените к компьютеру политику Kaspersky Security Center с установленными параметрами для расшифровки всех жестких дисков компьютера.

2. Запустите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Чтобы удалить данные о несовместимости программы с Агентом

аутентификации, в командной строке введите команду `avp pbatestreset`.

Управление BitLocker

BitLocker – встроенная в операционную систему Windows технология шифрования. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет контролировать и управлять Bitlocker с помощью Kaspersky Security Center. BitLocker шифрует логический том. Шифрование съемных дисков с помощью BitLocker невозможно. Подробнее о BitLocker см. в документации Microsoft.

BitLocker обеспечивает безопасность хранения ключей доступа с помощью доверенного платформенного модуля. Доверенный платформенный модуль (англ. Trusted Platform Module – TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины. Использование TPM является самым безопасным способом хранения ключей доступа BitLocker, так как TPM позволяет проверять целостность операционной системы. На компьютерах без TPM вы также можете зашифровать диски. При этом ключ доступа будет зашифрован паролем. Таким образом, BitLocker использует следующие способы аутентификации:

- TPM и пароль.
- TPM и PIN-код.
- Пароль.

После шифрования диска BitLocker создает мастер-ключ. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправляет мастерключ в Kaspersky Security Center, чтобы вы имели возможность восстановить доступ к диску, если пользователь, например, забыл пароль. Если пользователь самостоятельно зашифровал диск с помощью BitLocker, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправит информацию о шифровании диска в Kaspersky Security Center. При этом Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не отправит мастер-ключ в Kaspersky Security Center, и восстановить доступ к диску с помощью Kaspersky Security Center будет невозможно. Для корректной работы BitLocker с Kaspersky Security Center расшифруйте диск и зашифруйте диск повторно с помощью политики. Расшифровать диск вы можете локально или с помощью политики.

После шифрования системного жесткого диска для загрузки операционной системы пользователю нужно пройти процедуру аутентификации BitLocker. После прохождения процедуры аутентификации BitLocker будет доступен вход в систему. BitLocker не поддерживает технологию единого входа (SSO).

Если вы используете групповые политики для Windows, выключите управление BitLocker в параметрах политики. Параметры политики для Windows могут противоречить параметрам политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. При шифровании диска могут возникнуть ошибки.

Запуск шифрования диска BitLocker

Перед запуском полнодискового шифрования рекомендуется убедиться в том, что компьютер не заражен. Для этого запустите полную проверку или проверку важных областей компьютера. Выполнение полнодискового шифрования на компьютере, зараженном руткитом, может привести к неработоспособности компьютера.

Для работы BitLocker на компьютерах под управлением операционной системы Windows для серверов может потребоваться установить компонент шифрования диска BitLocker. Установите компонент средствами операционной системы (мастер добавления ролей и компонентов). Подробнее об установке компонента шифрования диска BitLocker см. в документации Microsoft.

Как запустить шифрование диска BitLocker через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Полнодисковое шифрование.
6. В раскрывающемся списке Технология шифрования выберите элемент Шифрование диска BitLocker.
7. В раскрывающемся списке Режим шифрования выберите элемент Шифровать все жесткие диски.

   Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой выполнялось шифрование.
8. Настройте дополнительные параметры шифрования диска BitLocker (см. таблицу ниже).
9. Сохраните внесенные изменения.

Как запустить шифрование диска BitLocker через Web Console

1. В главном окне Web Console выберите закладку Устройства → Политики и профили политик.
2. Нажмите на название политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для компьютеров, на которых вы хотите запустить шифрование диска BitLocker.

   Откроется окно свойств политики.
3. Выберите закладку Параметры программы.
4. Перейдите в раздел Шифрование данных → Полнодисковое шифрование.
5. В блоке Управление шифрованием выберите элемент Шифрование диска BitLocker.
6. Перейдите на ссылке Шифрование диска BitLocker.

   Откроется окно с параметрами шифрования диска BitLocker.
7. В раскрывающемся списке Режим шифрования выберите элемент Шифровать все жесткие диски.

   Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой выполнялось шифрование.
8. Настройте дополнительные параметры шифрования диска BitLocker (см. таблицу ниже).
9. Нажмите на кнопку OK.

После применения политики на клиентском компьютере с установленной программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready появятся следующие запросы:

- При наличии модуля TPM, появится окно запроса PIN-кода.
- При отсутствии модуля TPM, появится окно запроса пароля для предзагрузочной аутентификации.
- Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), то в операционных системах Windows 8, а также в более ранних версиях появится окно запроса на подключение запоминающего устройства для сохранения файла ключа восстановления. Вы можете сохранять несколько файлов ключей восстановления на одном запоминающем устройстве.

После установки пароля или PIN-кода BitLocker запросит перезагрузку компьютера для завершения шифрования диска. Далее пользователю нужно пройти процедуру аутентификации BitLocker. После прохождения процедуры аутентификации BitLocker нужно выполнить вход в систему. После загрузки операционной системы BitLocker завершит шифрование диска.

При отсутствии доступа к ключам шифрования пользователь может запросить у администратора локальной сети организации ключ восстановления (если ключ восстановления не был сохранен ранее на запоминающем устройстве или был утерян).

Параметры компонента Шифрование диска BitLocker

Параметр	Описание

Включить использование проверки подлинности BitLocker, требующей предзагрузочного ввода с клавиатуры на планшетах	Флажок включает / выключает использование аутентификации, требующей ввода данных в предзагрузочной среде, даже если у платформы отсутствует возможность предзагрузочного ввода (например, у сенсорных клавиатур на планшетах). Сенсорная клавиатура планшетов недоступна в предзагрузочной среде. Для прохождения аутентификации BitLocker на планшетах пользователю необходимо подключить, например, USB-клавиатуру. Если флажок установлен, то использование аутентификации, требующей предзагрузочного ввода, разрешено. Рекомендуется использовать этот параметр только для устройств, у которых во время предварительной загрузки, помимо сенсорных клавиатур, имеются альтернативные средства ввода данных, например, USB-клавиатура. Если флажок снят, шифрование диска BitLocker на планшетах невозможно.
Использовать аппаратное шифрование	Если флажок установлен, то программа применяет аппаратное шифрование. Это позволяет увеличить скорость шифрования и сократить использование ресурсов компьютера.
Шифровать только занятое пространство	Флажок включает / выключает функцию, ограничивающую область шифрования только занятыми секторами жесткого диска. Это ограничение позволяет сократить время шифрования. Включение / выключение функции Шифровать только занятое пространство после запуска шифрования не изменяет этого параметра до тех пор, пока жесткие диски не будут расшифрованы. Требуется установить или снять флажок до начала шифрования. Если флажок установлен, то шифруется только та часть жесткого диска, которая занята файлами. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь жесткий диск, в том числе остатки удаленных и отредактированных ранее файлов. Данную функцию рекомендуется применять для новых жестких дисков, данные которых не редактировались и не удалялись. Если вы применяете шифрование на уже используемом жестком диске, рекомендуется зашифровать весь жесткий диск. Это гарантирует защиту всех данных – даже удаленных, но потенциально восстанавливаемых. По умолчанию флажок снят.

Параметры аутентификации	Использовать доверенный платформенный модуль (TPM) Если выбран этот вариант, BitLocker использует доверенный платформенный модуль (TPM). Доверенный платформенный модуль (англ. Trusted Platform Module – TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины. Для компьютеров под управлением операционных систем Windows 7 и Windows Server 2008 R2 доступно только шифрование с использованием модуля TPM. Если модуль TPM не установлен, шифрование BitLocker невозможно. Использование пароля на этих компьютерах не поддерживается. Устройство, оснащенное доверенным платформенным модулем, может создавать ключи шифрования, которые могут быть расшифрованы только с его помощью. Доверенный платформенный модуль шифрует ключи шифрования собственным корневым ключом хранилища. Корневой ключ хранилища хранится внутри доверенного платформенного модуля. Это обеспечивает дополнительную степень защиты ключей шифрования от попыток взлома. Этот вариант действия выбран по умолчанию. Вы можете настроить параметры доступа к ключу шифрования: • Использовать PIN-код. Если флажок установлен, пользователь может использовать PIN-код для получения доступа к ключу шифрования, который хранится в доверенном платформенном модуле (TPM). Если флажок снят, пользователю запрещено использовать PIN-код. Для получения доступа к ключу шифрования пользователь использует пароль. • Использовать пароль, если доверенный платформенный модуль (TPM) недоступен. Если флажок установлен, то при отсутствии доверенного платформенного модуля (TPM) пользователь может получить доступ к ключам шифрования с помощью пароля. Если флажок снят и модуль TPM недоступен, то полнодисковое шифрование не запускается. Использовать пароль Если выбран этот вариант, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready запрашивает у пользователя пароль при обращении к зашифрованному диску. Этот вариант действия может быть выбран, если не используется доверенный платформенный модуль (TPM).

Расшифровка жесткого диска, защищенного BitLocker

Пользователь может самостоятельно расшифровать диск средствами операционной системы (функция Выключение BitLocker). После этого, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предложит зашифровать диск повторно. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет предлагать зашифровать диск пока вы не включите расшифровку дисков в политике.

Как расшифровать жесткий диск, защищенный BitLocker, через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Полнодисковое шифрование.
6. В раскрывающемся списке Технология шифрования выберите элемент Шифрование диска BitLocker.
7. В раскрывающемся списке Режим шифрования выберите элемент Расшифровывать все жесткие диски.
8. Сохраните внесенные изменения.

Как расшифровать жесткий диск, защищенный BitLocker, через Web Console

1. В главном окне Web Console выберите закладку Устройства → Политики и профили политик.
2. Нажмите на название политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для компьютеров, на которых вы хотите расшифровать жесткие диски.

Откроется окно свойств политики.

3. Выберите закладку Параметры программы.
4. Перейдите в раздел Шифрование данных → Полнодисковое шифрование.
5. Выберите технологию Шифрование диска BitLocker и перейдите по ссылке для настройки параметров.

Откроются параметры шифрования.

6. В раскрывающемся списке Режим шифрования выберите элемент Расшифровывать все жесткие диски.
7. Нажмите на кнопку OK.

Восстановление доступа к диску, защищенному BitLocker

Если пользователь забыл пароль доступа к жесткому диску, зашифрованному BitLocker, нужно запустить процедуру восстановления ("Запрос - Ответ").

Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), то для операционных систем Windows 8, а также в более ранних версий, файл ключа восстановления был сохранен на съемный диск перед шифрованием. Для восстановления доступа к диску вставьте съемный диск и следуйте инструкциям на экране.

Восстановление доступа к жесткому диску, зашифрованному BitLocker, состоит из следующих этапов:

1. Пользователь сообщает администратору идентификатор ключа восстановления (см. рис. ниже).

2. Администратор проверяет идентификатор ключа восстановления в свойствах компьютера в Kaspersky Security Center. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в свойствах компьютера.

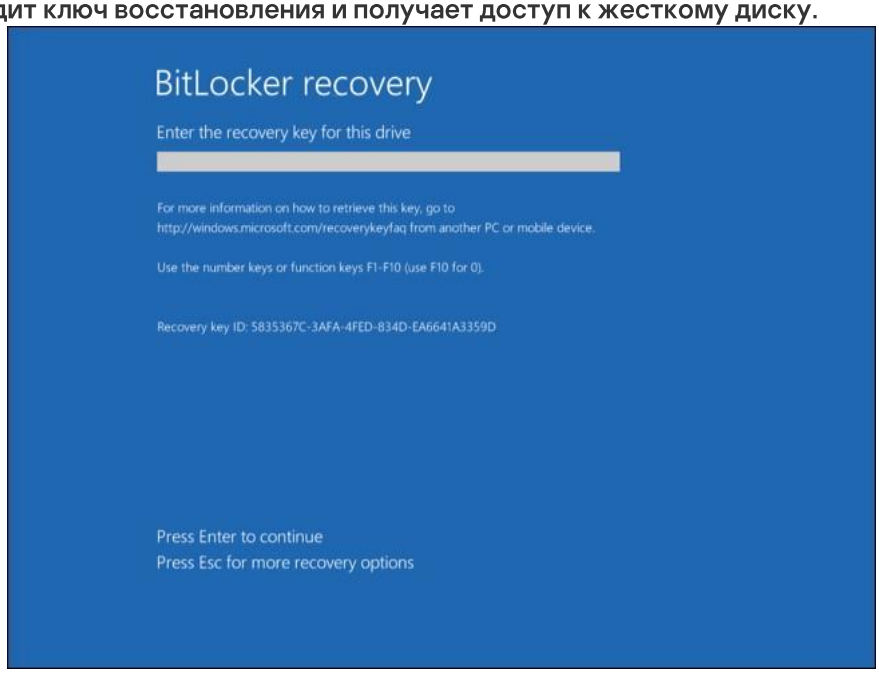
3. Если идентификаторы ключа восстановления совпадают, администратор сообщает пользователю ключ восстановления или передает файл ключа восстановления.

   Файл ключа восстановления используется для компьютеров под управлением следующих операционных систем:

   - Windows 7;
   - Windows 8;
   - Windows Server 2008;
   - Windows Server 2011;
   - Windows Server 2012.

   Для остальных операционных систем используется ключ восстановления.

4. Пользователь вводит ключ восстановления и получает доступ к жесткому диску.



Восстановление доступа к системному диску

Для запуска процедуры восстановления пользователю нужно на этапе предзагрузочной аутентификации нажать клавишу Esc.

Как просмотреть ключ восстановления для системного диска, зашифрованного BitLocker, в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Устройства.
4. На закладке Устройства выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт Предоставление доступа в офлайн-режиме.
6. В открывшемся окне выберите закладку Доступ к системному диску с защитой BitLocker.
7. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле Идентификатор ключа восстановления.

   Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

В результате вам будет доступен ключ восстановления или файл ключа восстановления, который нужно будет передать пользователю.

Как просмотреть ключ восстановления для системного диска, зашифрованного BitLocker, в Web Console

1. В главном окне Web Console выберите Устройства → Управляемые устройства.
2. Установите флажок рядом с именем компьютера, доступ к диску которого вы хотите восстановить.
3. Нажмите на кнопку Предоставить доступ к устройству в автономном режиме.
4. В открывшемся окне выберите раздел BitLocker.
5. Проверьте идентификатор ключа восстановления. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в параметрах компьютера.

   Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.
6. Нажмите на кнопку Получить ключ.

В результате вам будет доступен ключ восстановления или файл ключа восстановления, который нужно будет передать пользователю.

После загрузки операционной системы пользователю нужно сменить пароль. Для этого пользователю нужно открыть Панель управления операционной системы и перейти в параметры BitLocker. В параметрах BitLocker пользователю нужно сбросить старый пароль и задать новый. Если пользователь не сменил пароль, при следующей загрузке операционной системы вы можете использовать старый ключ восстановления.

Восстановление доступа к несистемному диску

Для запуска процедуры восстановления пользователю нужно в окне предоставления доступа к диску перейти по ссылке Забыли пароль. После получения доступа к зашифрованному диску пользователь может включить автоматическую разблокировку диска при аутентификации Windows в параметрах BitLocker.

Как просмотреть ключ восстановления для несистемного диска, зашифрованного BitLocker, в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку Дополнительно → Шифрование и защита данных → Зашифрованные устройства.
3. В рабочей области выберите зашифрованное устройство, для которого вы хотите создать файл ключа доступа, и в контекстном меню устройства выберите пункт Получить доступ к устройству в Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).
4. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле Идентификатор ключа восстановления.

   Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.
5. Передайте пользователю ключ, указанный в поле Ключ восстановления.

Как просмотреть ключ восстановления для несистемного диска, зашифрованного BitLocker, в Web Console

1. В главном окне Web Console выберите Операции → Шифрование и защита данных → Зашифрованные устройства.
2. Установите флажок рядом с именем компьютера, доступ к диску которого вы хотите восстановить.
3. Нажмите на кнопку Предоставить доступ к устройству в автономном режиме.

   Запустится мастер предоставления доступа к устройству.
4. Следуйте указаниям мастера предоставления доступа к устройству:
   a. Выберите плагин Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows.
   b. Проверьте идентификатор ключа восстановления. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в параметрах компьютера.

      Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.
   c. Нажмите на кнопку Получить ключ.

В результате вам будет доступен ключ восстановления или файл ключа восстановления, который нужно будет передать пользователю.

Шифрование файлов на локальных дисках компьютера

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для

рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Шифрование файлов имеет следующие особенности:

- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready шифрует / расшифровывает стандартные папки только для локальных профилей пользователей (англ. local user pro les) операционной системы. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не шифрует и не расшифровывает стандартные папки для перемещаемых профилей пользователей (англ. roaming user pro les), обязательных профилей пользователей (англ. mandatory user pro les), временных профилей пользователей (англ. temporary user pro les), а также перенаправленные папки.

- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не выполняет шифрование файлов, изменение которых может повредить работе операционной системы и установленных программ. Например, в список исключений из шифрования входят следующие файлы и папки со всеми вложенными в них папками:

  - %WINDIR%;
  - %PROGRAMFILES% и %PROGRAMFILES(X86)%;
  - файлы реестра Windows.

  Список исключений из шифрования недоступен для просмотра и изменения. Файлы и папки из списка исключений из шифрования можно добавить в список для шифрования, но при выполнении шифрования файлов они не будут зашифрованы.

Запуск шифрования файлов на локальных дисках компьютера

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не шифрует файлы, содержимое которых расположено в облачном хранилище OneDrive, и блокирует копирование зашифрованных файлов в облачное хранилище OneDrive, если эти файлы не добавлены в правило расшифровки.

Чтобы зашифровать файлы на локальных дисках компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Шифрование файлов.
6. В правой части окна выберите закладку Шифрование.
7. В раскрывающемся списке Режим шифрования выберите элемент Согласно правилам.

8. На закладке Шифрование нажмите на кнопку Добавить и в раскрывающемся списке выберите один из следующих элементов:

   a. Выберите элемент Стандартные папки, чтобы добавить в правило шифрования файлы из папок локальных профилей пользователей, предложенных специалистами "Лаборатории Касперского".

   - Документы. Файлы в стандартной папке операционной системы Документы, а также вложенные папки.
   - Избранное. Файлы в стандартной папке операционной системы Избранное, а также вложенные папки.
   - Рабочий стол. Файлы в стандартной папке операционной системы Рабочий стол, а также вложенные папки.
   - Временные файлы. Временные файлы, связанные с работой установленных на компьютере программ. Например, программы Microsoft O ice создают временные файлы с резервными копиями документов.
   - Файлы Outlook. Файлы, связанные с работой почтового клиента Outlook: файлы данных (PST), автономные файлы данных (OST), файлы автономной адресной книги (OAB) и файлы персональной адресной книги (PAB).

   b. Выберите элемент Папку вручную, чтобы добавить в правило шифрования папку, путь к которой введен вручную.

   При добавлении пути к папке следует использовать следующие правила:

   - Используйте переменную окружения (например, `%FOLDER%\UserFolder\`). Вы можете использовать переменную окружения только один раз и только в начале пути.
   - Не используйте относительные пути. Вы можете использовать набор `\..\` (например, `C:\Users\..\UserFolder\`). Набор `\..\` обозначает переход к родительской папке.
   - Не используйте символы `*` и `?`.
   - Не используйте UNC-пути.
   - Используйте `;` или `,` в качестве разделительного символа.

   c. Выберите элемент Файлы по расширению, чтобы добавить в правило шифрования отдельные расширения файлов. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует файлы с указанными расширениями на всех локальных дисках компьютера.

   d. Выберите элемент Файлы по группам расширений, чтобы добавить в правило шифрования группы расширений файлов (например, группа Документы Microsoft O ice). Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует файлы с расширениями, перечисленными в группах расширений, на всех локальных дисках компьютера.

9. Сохраните внесенные изменения.

Сразу после применения политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует файлы, включенные в правило шифрования и не включенные в правило расшифровки.

Шифрование файлов имеет следующие особенности:

- Если один и тот же файл добавлен и в правило шифрования, и в правило расшифровки, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready выполняет следующие действия:

Если исходный файл не зашифрован, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не шифрует этот файл.

- Если исходный файл зашифрован, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready расшифровывает этот файл.

- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready продолжает шифровать новые файлы, если файлы удовлетворяют критериям правила шифрования. Например, вы изменили свойства незашифрованного файла (путь или расширение), и в результате файл удовлетворяет критериям правила шифрования. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready шифрует этот файл.

- Когда пользователь создает новый файл, свойства которого удовлетворяют критериям правила шифрования, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready шифрует файл сразу же при открытии файла.

- Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready откладывает шифрование открытых файлов до тех пор, пока они не будут закрыты.

- Если вы переносите зашифрованный файл в другую папку на локальном диске, файл остается зашифрованным, независимо от того, включена ли эта папка в правило шифрования.

- Если вы расшифровали файл и скопировали файл в другую папку на локальном диске, которая не включена в правило расшифровки, копия файла может быть зашифрована. Для исключения шифрования копии файла, создайте для целевой папки правило расшифровки.

Формирование правил доступа программ к зашифрованным файлам

Чтобы сформировать правила доступа программ к зашифрованным файлам, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Шифрование файлов.
6. В раскрывающемся списке Режим шифрования выберите элемент Согласно правилам.

Правила доступа действуют только в режиме Согласно правилам. Если после применения правил доступа в режиме Согласно правилам вы перейдете в режим Оставлять без изменений, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready будет игнорировать все правила доступа. Все программы будут иметь доступ ко всем зашифрованным файлам.

7. В правой части окна выберите закладку Правила для программ.

8. Если вы хотите выбрать программы исключительно из списка Kaspersky Security Center, нажмите на кнопку Добавить и в раскрывающемся списке выберите элемент Программы из списка Kaspersky Security Center.

   a. Задайте фильтры для вывода списка программ в таблице. Для этого укажите значения параметров Программа, Производитель, Период добавления, а также флажков из блока Группа. b. Нажмите на кнопку Обновить.

   c. В таблице отобразится список программ, удовлетворяющих заданным фильтрам.

   d. В графе Программы установите флажки напротив тех программ в таблице, для которых вы хотите сформировать правила доступа к зашифрованным файлам.

   e. В раскрывающемся списке Правило для программ выберите правило, которое будет определять доступ программ к зашифрованным файлам.

   f. В раскрывающемся списке Действие для программ, выбранных ранее выберите действие, которое выполняет Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready над правилами доступа к зашифрованным файлам, сформированными для указанных выше программ ранее.

   g. Нажмите на кнопку OK.

   Информация о правиле доступа программ к зашифрованным файлам отобразится в таблице на закладке Правила для программ.

9. Если вы хотите выбрать программы вручную, нажмите на кнопку Добавить и в раскрывающемся списке выберите элемент Программы вручную.

   a. В поле ввода введите имя или список имен исполняемых файлов программ с их расширениями.

      Вы можете также добавить имена исполняемых файлов программ из списка Kaspersky Security Center, нажав на кнопку Добавить из списка Kaspersky Security Center.

   b. Если требуется, в поле Описание введите описание списка программ.

   c. В раскрывающемся списке Правило для программ выберите правило, которое будет определять доступ программ к зашифрованным файлам.

   d. Нажмите на кнопку OK.

   Информация о правиле доступа программ к зашифрованным файлам отобразится в таблице на закладке Правила для программ.

10. Сохраните внесенные изменения.

Шифрование файлов, создаваемых и изменяемых отдельными программами

Вы можете создать правило, согласно которому Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет шифровать все файлы, создаваемые и изменяемые указанными в правиле программами.

Файлы, созданные или измененные указанными программами до применения правила шифрования, не будут зашифрованы.

Чтобы настроить шифрование файлов, создаваемых и изменяемых отдельными программами, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Шифрование файлов.
6. В раскрывающемся списке Режим шифрования выберите элемент Согласно правилам.

   Правила шифрования действуют только в режиме Согласно правилам. Если после применения правил шифрования в режиме Согласно правилам вы перейдете в режим Оставлять без изменений, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет игнорировать все правила шифрования. Файлы, которые были зашифрованы ранее, по-прежнему останутся зашифрованными.

7. В правой части окна выберите закладку Правила для программ.
8. Если вы хотите выбрать программы исключительно из списка Kaspersky Security Center, нажмите на кнопку Добавить и в раскрывающемся списке выберите элемент Программы из списка Kaspersky Security Center.

   Откроется окно Добавление программ из списка Kaspersky Security Center.

   Выполните следующие действия:

   a. Задайте фильтры для вывода списка программ в таблице. Для этого укажите значения параметров Программа, Производитель, Период добавления, а также флажков из блока Группа. b. Нажмите на кнопку Обновить.

      В таблице отобразится список программ, удовлетворяющих заданным фильтрам.

   c. В графе Программы установите флажки напротив тех программ в таблице, создаваемые файлы которых вы хотите шифровать.

   d. В раскрывающемся списке Правило для программ выберите элемент Шифровать все создаваемые файлы.

e. В раскрывающемся списке Действие для программ, выбранных ранее выберите действие, которое выполняет Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready над правилами шифрования файлов, сформированными для указанных выше программ ранее.

f. Нажмите на кнопку OK.

Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными программами, отобразится в таблице на закладке Правила для программ.

9. Если вы хотите выбрать программы вручную, нажмите на кнопку Добавить и в раскрывающемся списке выберите элемент Программы вручную.

Откроется окно Добавление / изменение названий исполняемых файлов программ.

Выполните следующие действия:

a. В поле ввода введите имя или список имен исполняемых файлов программ с их расширениями.

Вы можете также добавить имена исполняемых файлов программ из списка Kaspersky Security Center, нажав на кнопку Добавить из списка Kaspersky Security Center.

b. Если требуется, в поле Описание введите описание списка программ.

c. В раскрывающемся списке Правило для программ выберите элемент Шифровать все создаваемые файлы.

d. Нажмите на кнопку OK.

Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными программами, отобразится в таблице на закладке Правила для программ.

10. Сохраните внесенные изменения.

Формирование правила расшифровки

Чтобы сформировать правило расшифровки, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку Политики.

4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

5. В окне политики выберите Шифрование данных → Шифрование файлов.

6. В правой части окна выберите закладку Расшифровка.

7. В раскрывающемся списке Режим шифрования выберите элемент Согласно правилам.

8. На закладке Расшифровка нажмите на кнопку Добавить и в раскрывающемся списке выберите один из следующих элементов:

   a. Выберите элемент Стандартные папки, чтобы добавить в правило расшифровки файлы из папок локальных профилей пользователей, предложенных специалистами "Лаборатории Касперского".

   b. Выберите элемент Папку вручную, чтобы добавить в правило расшифровки папку, путь к которой введен вручную.

   c. Выберите элемент Файлы по расширению, чтобы добавить в правило расшифровки отдельные расширения файлов. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не шифрует файлы с указанными расширениями на всех локальных дисках компьютера.

   d. Выберите элемент Файлы по группам расширений, чтобы добавить в правило расшифровки группы расширений файлов (например, группа Документы Microsoft O ice). Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не шифрует файлы с расширениями, перечисленными в группах расширений, на всех локальных дисках компьютера.

9. Сохраните внесенные изменения.

Если один и тот же файл добавлен и в правило шифрования, и в правило расшифровки, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не шифрует этот файл, если он не зашифрован, и расшифровывает, если он зашифрован.

Расшифровка файлов на локальных дисках компьютера

Чтобы расшифровать файлы на локальных дисках компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку Политики.

4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

5. В окне политики выберите Шифрование данных → Шифрование файлов.

6. В правой части окна выберите закладку Шифрование.

7. Исключите из списка для шифрования файлы и папки, которые вы хотите расшифровать. Для этого в списке выберите файлы и в контекстном меню кнопки Удалить выберите пункт Удалить правило и расшифровать файлы.

   Вы можете удалять сразу несколько элементов из списка для шифрования. Для этого, удерживая клавишу CTRL, левой клавишей мыши выберите нужные элементы и в контекстном меню кнопки Удалить выберите пункт Удалить правило и расшифровать файлы.

   Удаленные из списка для шифрования файлы и папки автоматически добавляются в список для расшифровки.

8. Сформируйте список файлов для расшифровки.

9. Сохраните внесенные изменения.

Сразу после применения политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready расшифровывает зашифрованные файлы, добавленные в список для расшифровки.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready расшифровывает зашифрованные файлы, если их параметры (путь к файлу / название файла / расширение файла) изменяются и начинают удовлетворять параметрам объектов, добавленных в список для расшифровки.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready откладывает расшифровку открытых файлов до тех пор, пока они не будут закрыты.

Создание зашифрованных архивов

Для защиты данных при передаче файлов пользователям вне корпоративной сети вы можете использовать зашифрованные архивы. Зашифрованные архивы удобно использовать для передачи файлов большого размера с помощью съемных дисков, так как почтовые клиенты имеют ограничения по размеру файла.

Перед созданием зашифрованных архивов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запросит у пользователя пароль. Для обеспечения надежной защиты данных вы можете включить проверку сложности паролей и выбрать критерии сложности. Таким образом, пользователю будет запрещено использовать короткие и простые пароли, например, 1234.

Как включить проверку сложности пароля при создании зашифрованных архивов в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Общие параметры шифрования.
6. В блоке Параметры паролей нажмите на кнопку Настройка.
7. В открывшемся окне выберите закладку Зашифрованные архивы.
8. Настройте параметры сложности пароля при создании зашифрованных архивов.

Как включить проверку сложности пароля при создании зашифрованных архивов в Web Console

1. В главном окне Web Console выберите закладку Устройства → Политики и профили политик.
2. Нажмите на название политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для компьютеров, на которых вы хотите включить проверку сложности паролей.

Откроется окно свойств политики.

3. Выберите закладку Параметры программы.

4. Перейдите в раздел Шифрование данных → Шифрование файлов.

5. В блоке Параметры пароля для зашифрованных архивов настройте параметры сложности пароля при создании зашифрованных архивов.

Вы можете создавать зашифрованные архивы на компьютерах с установленной программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с функцией шифрования файлов.

При добавлении в зашифрованный архив файла, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready загружает содержимое этого файла и осуществляет шифрование.

Чтобы создать зашифрованный архив, выполните следующие действия:

1. В любом файловом менеджере выделите файлы или папки, которые вы хотите добавить в зашифрованный архив. По правой клавише мыши откройте их контекстное меню.

2. Выберите пункт Создать зашифрованный архив в контекстном меню (см. рис. ниже).

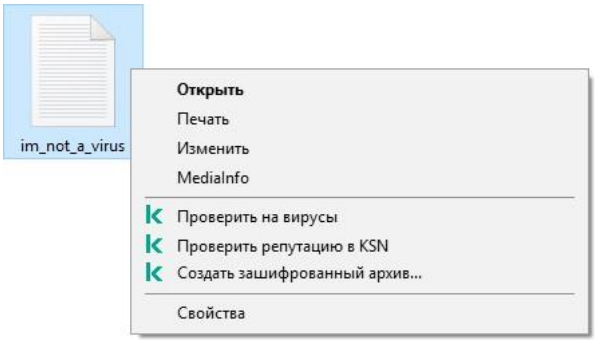
3. В открывшемся окне выберите место для сохранения зашифрованного архива на съемном диске, задайте имя и нажмите на кнопку Сохранить.

4. В открывшемся окне задайте пароль и повторите его.

   Пароль должен соответствовать критериям сложности, заданным в политике.

5. Нажмите на кнопку Создать.

Запустится процесс создания зашифрованного архива. В процессе создания зашифрованного архива Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не выполняет сжатие файлов. По завершении процесса в указанном месте на диске будет создан самораспаковывающийся защищенный паролем зашифрованный архив (исполняемый файл с расширением exe) – .



Создание зашифрованного архива

Для получения доступа к файлам в зашифрованном архиве нужно запустить мастер распаковки архива двойным щелчком мыши и ввести пароль. Если вы забыли пароль, восстановить доступ к файлам в зашифрованном архиве невозможно. Вы можете создать зашифрованный архив повторно.

Восстановление доступа к зашифрованными файлам

При шифровании файлов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready получает ключ шифрования, необходимый для прямого доступа к зашифрованным файлам. С помощью ключа шифрования пользователь, работающий под любой из учетных записей Windows, которая была активной во время шифрования файлов, может получать прямой доступ к зашифрованным файлам. Пользователям, работающим под учетными записями Windows, которые были неактивны во время шифрования файлов, требуется связь с Kaspersky Security Center для доступа к зашифрованным файлам.

Зашифрованные файлы могут быть недоступны в следующих случаях:

- На компьютере пользователя присутствуют ключи шифрования, но нет связи с Kaspersky Security Center для работы с ними. В этом случае пользователю требуется запросить доступ к зашифрованным файлам у администратора локальной сети организации.

  При отсутствии связи с Kaspersky Security Center требуется:

  - для доступа к зашифрованным файлам на жестких дисках компьютера запросить один ключ доступа;
  -

  для доступа к зашифрованным файлам на съемных дисках запросить ключ доступа к зашифрованным файлам для каждого съемного диска.

- С компьютера пользователя удалены компоненты шифрования. В этом случае пользователь может открыть зашифрованные файлы на локальных дисках и съемных дисках, но содержимое файлов отображается как зашифрованное.

  Пользователь может работать с зашифрованными файлами при следующих условиях:

  - Файлы помещены в зашифрованные архивы, созданные на компьютере с установленной программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

  - Файлы хранятся на съемных дисках, для которых разрешена работа в портативном режиме.

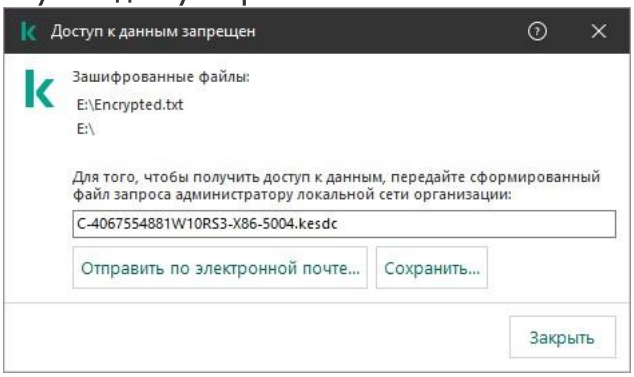
Для получения доступ к зашифрованным файлам пользователю нужно запустить процедуру восстановления ("Запрос - Ответ").

Восстановление доступ к зашифрованным файлам состоит из следующих этапов:

1. Пользователь отправляет администратору файл запроса (см. рис. ниже).

2. Администратор добавляет файл запроса в Kaspersky Security Center, создает файл ключа доступа и отправляет файл пользователю.

3. Пользователь добавляет файл ключа доступа в Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и получает доступ к файлам.



Для запуска процедуры восстановления пользователю нужно обратиться к файлу. В результате Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создаст файл запроса (файл с расширением kesdc), который пользователю нужно передать администратору, например, по электронной почте.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready формирует файл запроса доступа ко всем зашифрованным файлам, хранящимся на диске компьютера (локальном диске или съемном диске).

Как получить файл ключа доступа к зашифрованным данным в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Устройства.
4. На закладке Устройства выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт Предоставление доступа в офлайн-режиме.
6. В открывшемся окне выберите закладку Шифрование данных.
7. На закладке Шифрование данных нажмите на кнопку Обзор.
8. В окне выбора файла запроса укажите путь к файлу, полученного от пользователя.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.

Как получить файл ключа доступа к зашифрованным данным в Web Console

1. В главном окне Web Console выберите Устройства → Управляемые устройства.
2. Установите флажок рядом с именем компьютера, доступ к данным которого вы хотите восстановить.
3. Нажмите на кнопку Предоставить доступ к устройству в автономном режиме.
4. Выберите раздел Шифрование данных.
5. Нажмите на кнопку Выбрать файл и выберите файл запроса, полученный от пользователя (файл с расширением kesdc).

Web Console покажет информацию о запросе. В том числе, имя компьютера, на котором пользователь запрашивает доступ к файлу.

6. Нажмите на кнопку Сохранить ключ и выберите папку для сохранения файла ключа доступа к зашифрованным данным (файл с расширением kesdr).

В результате вам будет доступен ключ доступа к зашифрованным данным, который нужно будет передать пользователю.

После получения файла ключа доступа к зашифрованным данным пользователю нужно запустить файл двойным щелчком мыши. В результате Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предоставит доступ ко всем зашифрованным файлам, хранящимся диске. Для получения доступа к зашифрованным файлам, хранящимся на других дисках, требуется получить отдельные ключи доступа для этих дисков.

Восстановление доступа к зашифрованным данным в случае выхода из строя операционной системы

Восстановление доступа к данным в случае выхода из строя операционной системы доступно только при шифровании файлов (FLE). Восстановить доступ к данным при полнодисковом шифровании (FDE) невозможно.

Чтобы восстановить доступ к зашифрованным данным в случае выхода из строя операционной системы, выполните следующие действия:

1. Переустановите операционную систему, не форматируя жесткий диск.
2. Установите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
3. Установите связь между компьютером и Сервером администрирования Kaspersky Security Center, под управлением которого находился компьютер во время шифрования данных.

Доступ к зашифрованным данным будет предоставлен на тех же условиях, которые действовали до выхода операционной системы из строя.

Изменение шаблонов сообщений для получения доступа к зашифрованным файлам

Чтобы изменить шаблоны сообщений для получения доступа к зашифрованным файлам, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Общие параметры шифрования.

6. В блоке Шаблоны нажмите на кнопку Шаблоны.

   Откроется окно Шаблоны.

7. Выполните следующие действия:

   - Если вы хотите изменить шаблон сообщения пользователя, выберите закладку Сообщение пользователя. Когда пользователь обращается к зашифрованному файлу при отсутствии на компьютере ключа доступа к зашифрованным файлам, открывается окно Доступ к данным запрещен. При нажатии на кнопку Отправить по электронной почте окна Доступ к данным запрещен автоматически формируется сообщение пользователя. Это сообщение отправляется администратору локальной сети организации вместе с файлом запроса доступа к зашифрованным файлам.

   - Если вы хотите изменить шаблон сообщения администратора, выберите закладку Сообщение администратора. Это сообщение автоматически формируется при нажатии на кнопку Отправить по электронной почте окна Запрос доступа к зашифрованным файлам и приходит к пользователю после предоставления ему доступа к зашифрованным файлам.

8. Измените шаблоны сообщений.

   Вы можете использовать кнопку По умолчанию и раскрывающийся список Переменная.

.

9 Сохраните внесенные изменения.

Шифрование съемных дисков

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает шифрование файлов в файловых системах FAT32 и NTFS. Если к компьютеру подключен съемный диск с неподдерживаемой файловой системой, то шифрование этого съемного диска завершается с ошибкой и Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready устанавливает статус доступа "только чтение" для этого съемного диска.

Для защиты данных на съемных дисках вы можете использовать следующие виды шифрования:

- Полнодисковое шифрование (англ. Full Disk Encryption – FDE).

  Шифрование всего съемного диска, включая файловую систему.

  Получить доступ к зашифрованным данным вне корпоративной сети невозможно. Также невозможно получить доступ к зашифрованным данным внутри корпоративной сети, если компьютер не подключен к Kaspersky Security Center ("гостевой" компьютер).

- Шифрование файлов (англ. File Level Encryption – FLE).

  Шифрование только файлов на съемном диске. Файловая система при этом остается без изменений.

  Шифрование файлов на съемных дисках предоставляет возможность доступа к данным за пределами корпоративной сети с помощью специального режима – портативный режим.

Во время шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает мастер-ключ. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет мастер-ключ в следующих хранилищах:

- Kaspersky Security Center.
- Компьютер пользователя.

  Мастер-ключ зашифрован секретным ключом пользователя.

- Съемный диск.

  Мастер-ключ зашифрован открытым ключом Kaspersky Security Center.

После завершения шифрования данные на съемном диске доступны внутри корпоративной сети как при использовании обычного съемного диска без шифрования.

Получение доступа к зашифрованным данным

При подключении съемного диска с зашифрованными данными Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

1. Проверяет наличие мастер-ключа в локальном хранилище на компьютере пользователя.

   Если мастер-ключ найден, пользователь получает доступ к данным на съемном диске.

   Если мастер-ключ не найден, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

   a. Отправляет запрос в Kaspersky Security Center.

      После получения запроса Kaspersky Security Center отправляет ответ, который содержит мастерключ.

   b. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет мастер-ключ в локальном хранилище на компьютере пользователя для дальнейшей работы с зашифрованным съемным диском.

2. Расшифровывает данные.

Особенности шифрования съемных дисков

Шифрование съемных дисков имеет следующие особенности:

- Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы управляемых компьютеров. Поэтому результат применения политики Kaspersky Security Center с настроенным шифрованием / расшифровкой съемных дисков зависит от того, к какому компьютеру подключен съемный диск.

- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не выполняет шифрование / расшифровку файлов со статусом доступа "только чтение", хранящихся на съемных дисках.

- В качестве съемных дисков поддерживаются следующие типы
  - устройств: носители информации, подключаемые по шине USB;
  - жесткие диски, подключаемые по шинам USB и FireWire; SSD-диски,
  - подключаемые по шинам USB и FireWire.

Запуск шифрования съемных дисков

Вы можете расшифровать съемный диск с помощью политики. Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы администрирования. Поэтому

.
результат расшифровки данных на съемных дисках зависит от того, к какому компьютеру подключен съемный диск.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает шифрование файловых систем FAT32 и NTFS. Если к компьютеру подключен съемный диск с неподдерживаемой файловой системой, шифрование съемного диска завершится с ошибкой и Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установит для этого съемного диска право доступа "только чтение".

Чтобы зашифровать съемные диски, выполните следующие действия:

1 Откройте Консоль администрирования Kaspersky Security Center.

2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку Политики.

4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

5. В окне политики выберите Шифрование данных → Шифрование съемных дисков.

6. В раскрывающемся списке Режим шифрования выберите действие, которое по умолчанию выполняет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready со съемными дисками:

   - Шифровать весь съемный диск (FDE). Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready посекторно шифрует содержимое съемного диска. Таким образом, зашифрованными оказываются не только файлы, которые хранятся на съемном диске, но и файловые системы, включая имена файлов и структуры папок на съемном диске.

   - Шифровать все файлы (FLE). Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует все файлы, которые хранятся на съемных дисках. Программа не шифрует файловые системы съемных дисков, включая имена файлов и структуры папок.

   - Шифровать только новые файлы (FLE). Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует только те файлы, которые были добавлены на съемные диски или которые хранились на съемных дисках и были изменены после последнего применения политики Kaspersky Security Center.

   Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready повторно не шифрует уже зашифрованный съемный диск.

7. Если вы хотите использовать портативный режим для шифрования съемных дисков, установите флажок Портативный режим.

   Портативный режим – режим шифрования файлов (FLE) на съемных дисках, который предоставляет возможность доступа к данным за пределами корпоративной сети. Также портативный режим позволяет работать с зашифрованными данными на компьютерах, на которых не установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

8. Если вы хотите зашифровать новый съемный диск, рекомендуется установить флажок Шифровать только занятое пространство. Если флажок снят, Kaspersky Endpoint Security для бизнеса -

Расширенный EDR Ready зашифрует все файлы, в том числе остатки удаленных или измененных файлов.

9. Если вы хотите настроить шифрование для отдельных съемных дисков, задайте правила шифрования.

10. Если вы хотите использовать полнодисковое шифрование съемных дисков в офлайн-режиме, установите флажок Разрешать шифрование съемных дисков в офлайн-режиме.

Офлайн-режим шифрования – режим шифрования съемных дисков (FDE) при отсутствии связи с Kaspersky Security Center. При шифровании Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет мастер-ключ только на компьютере пользователя. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправит мастер-ключ в Kaspersky Security Center при следующей синхронизации.

Если компьютер, на котором сохранен мастер-ключ, поврежден и данные в Kaspersky Security Center не отправлены, получить доступ к съемному диску невозможно.

Если флажок Разрешать шифрование съемных дисков в офлайн-режиме снят и подключение к Kaspersky Security Center отсутствует, шифрование съемного диска невозможно.

.

11 Сохраните внесенные изменения.

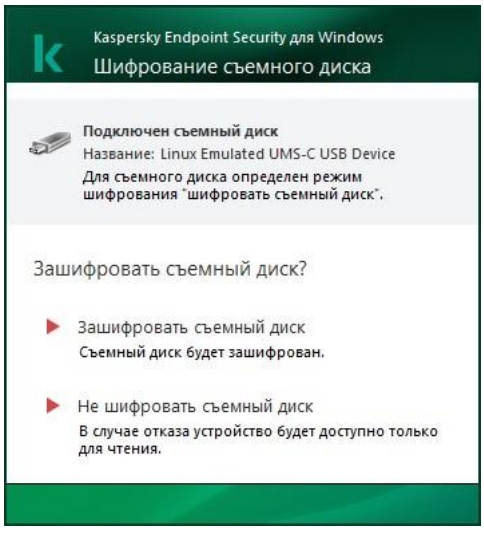
В результате применения политики, если пользователь подключает съемный диск или съемный диск уже подключен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запрашивает подтверждение для выполнения операции шифрования (см. рис. ниже).

Программа позволяет выполнить следующие действия:

- Если пользователь подтверждает запрос на шифрование, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует данные.
- Если пользователь отклоняет запрос на шифрование, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready оставляет данные без изменений и устанавливает для этого съемного диска право доступа "только чтение".
- Если пользователь не отвечает на запрос на шифрование, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready оставляет данные без изменений и устанавливает для этого съемного диска право доступа "только чтение". Программа повторно запрашивает подтверждение при последующем применении политики или при последующем подключении этого съемного диска.

Если во время шифрования данных пользователь инициирует безопасное извлечение съемного диска, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready прерывает шифрование данных и позволяет извлечь съемный диск до завершения операции шифрования. Шифрование данных будет продолжено при следующем подключении съемного диска к этому компьютеру.

Если шифрование съемного диска не удалось, просмотрите отчет Шифрование данных в интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Доступ к файлам может быть заблокирован другой программой. В этом случае попробуйте извлечь и заново подключить съемный диск к компьютеру.



Запрос на шифрование съемного диска

Добавление правила шифрования для съемных дисков

Чтобы добавить правило шифрования для съемных дисков, выполните следующие действия:

.

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3 В рабочей области выберите закладку Политики.

4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

5. В окне политики выберите Шифрование данных → Шифрование съемных дисков.

6. Нажмите на кнопку Добавить и в раскрывающемся списке выберите один из следующих элементов:

   - Если вы хотите добавить правила шифрования для съемных дисков, которые находятся в списке доверенных устройств компонента Контроль устройств, выберите элемент Из списка доверенных устройств данной политики.

   - Если вы хотите добавить правила шифрования для съемных дисков, которые находятся в списке Kaspersky Security Center, выберите элемент Из списка устройств Kaspersky Security Center.

7. В раскрывающемся списке Режим шифрования для выбранных устройств выберите действие, которое выполняет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с файлами, хранящимися на выбранных съемных дисках.

8. Установите флажок Портативный режим, если вы хотите, чтобы перед шифрованием Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполнял подготовку съемных дисков к работе с зашифрованными на них файлами в портативном режиме.

   Портативный режим позволяет работать с зашифрованными файлами съемных дисков на компьютерах с недоступной функциональностью шифрования.

9. Установите флажок Шифровать только занятое пространство, если вы хотите, чтобы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифровал только те секторы диска, которые заняты файлами.

   Если вы применяете шифрование на уже используемом диске, рекомендуется зашифровать весь диск. Это гарантирует защиту всех данных - даже удаленных, но еще содержащих извлекаемые сведения. Функцию Шифровать только занятое пространство рекомендуется использовать для новых, ранее не использовавшихся дисков.

   Если устройство было зашифровано ранее с использованием функции Шифровать только занятое пространство, после применения политики в режиме Шифровать весь съемный диск секторы, не занятые файлами, по-прежнему не будут зашифрованы.

10. В раскрывающемся списке Действие для устройств, выбранных ранее выберите действие, выполняемое Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с правилами шифрования, которые были определены для съемных дисков ранее:

    - Если вы хотите, чтобы созданное ранее правило шифрования съемного диска осталось без изменений, выберите элемент Пропустить.

    - Если вы хотите, чтобы созданное ранее правило шифрования съемного диска было заменено новым правилом, выберите элемент Обновить.

11. Сохраните внесенные изменения.

.

Добавленные правила шифрования съемных дисков будут применены к съемным дискам, подключенным к любым компьютерам организации.

Изменение правила шифрования для съемных дисков

Чтобы изменить правило шифрования для съемного диска, выполните следующие действия:

1 Откройте Консоль администрирования Kaspersky Security Center.

2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку Политики.

4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

5. В окне политики выберите Шифрование данных → Шифрование съемных дисков.

6. В списке съемных дисков, для которых определены правила шифрования, выберите запись о нужном вам съемном диске.

7. Нажмите на кнопку Задать правило, чтобы изменить правило шифрования для этого съемного диска.

   Откроется контекстное меню кнопки Задать правило.

8. В контекстном меню кнопки Задать правило выберите действие, которое выполняет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с файлами на выбранном съемном диске.

9. Сохраните внесенные изменения.

Измененные правила шифрования съемных дисков будут применены к съемным дискам, подключенным к любым компьютерам, работающим под управлением измененной политики Kaspersky Security Center.

Портативный режим для работы с зашифрованными файлами на съемных дисках

Портативный режим – режим шифрования файлов (FLE) на съемных дисках, который предоставляет возможность доступа к данным за пределами корпоративной сети. Также портативный режим позволяет работать с зашифрованными данными на компьютерах, на которых не установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Портативный режим удобно использовать в следующих случаях:

- Нет связи между компьютером и Сервером администрирования Kaspersky Security Center.
- Изменилась инфраструктура со сменой Сервера администрирования Kaspersky Security Center.
- На компьютере не установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

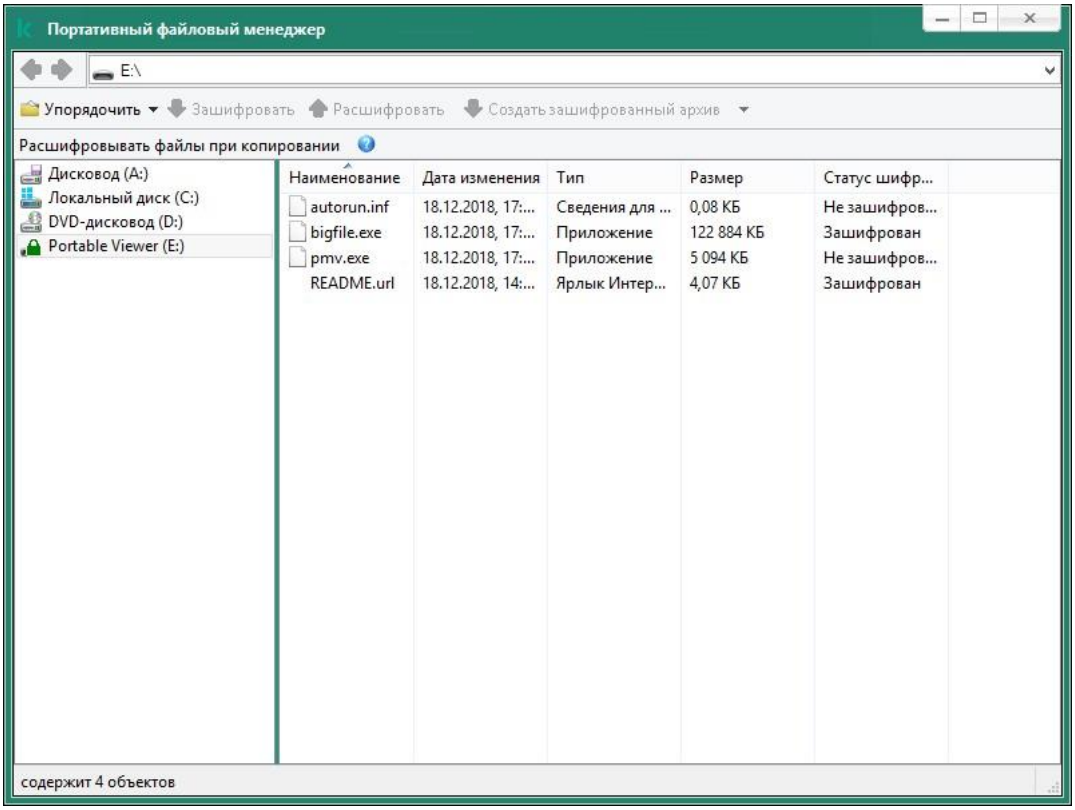
.

Портативный файловый менеджер

Для работы в портативном режиме Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready устанавливает на съемный диск специальный модуль шифрования – портативный файловый менеджер. Портативный файловый менеджер предоставляет интерфейс для работы с зашифрованными данными, если на компьютере не установлена программа
Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (см. рис. ниже). Если на компьютере установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, вы можете работать с зашифрованными съемными дисками с помощью обычных файлового менеджера (например, Проводника).

Портативный файловый менеджер хранит ключ для шифрования файлов на съемном диске. Ключ зашифрован паролем пользователя. Пользователь задает пароль перед шифрованием файлов на съемном диске.

Портативный файловый менеджер запускается автоматически при подключении съемного диска к компьютеру, на котором не установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если на компьютере выключен автозапуск программ, запустите портативный файловый менеджер вручную. Для этого запустите файл pmv.exe, который хранится на съемном диске.



Портативный файловый менеджер

Поддержка портативного режима для работы с зашифрованным файлами

Как включить поддержку портативного режима для работы с зашифрованными файлами на съемных дисках в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Шифрование съемных дисков.
6. В раскрывающемся списке Режим шифрования для выбранных устройств выберите элемент Шифровать все файлы или элемент Шифровать только новые файлы.

   Портативный режим доступен только при шифрования файлов (FLE). Включить поддержку портативного режима для полнодискового шифрования (FDE) невозможно.
7. Установите флажок Портативный режим.
8. Если нужно, добавьте правила шифрования для отдельных съемных дисков.
9. Сохраните внесенные изменения.
10. После применения политики подключите съемный диск к компьютеру.
11. Подтвердите операцию шифрования съемного диска.

    Откроется окно создания пароля для портативного файлового менеджера.
12. Задайте пароль, соответствующий требованиям к уровню сложности, и подтвердите его.
13. Нажмите на кнопку OK.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зашифрует файлы на съемном диске. Портативный файловый менеджер для работы с зашифрованными файлами будет также добавлен на съемный диск. Если на съемном диске уже есть зашифрованные файлы, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зашифрует их повторно с помощью собственного ключа. Это позволяет пользователю получить доступ ко всем файлам на съемном диске в портативном режиме.

Как включить поддержку портативного режима для работы с зашифрованными файлами на съемных дисках в Web Console

1. В главном окне Web Console выберите закладку Устройства → Политики и профили политик.
2. Нажмите на название политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для компьютеров, на которых вы хотите включить поддержку портативного режима.

   Откроется окно свойств политики.
3. Выберите закладку Параметры программы.
4. Перейдите в раздел Шифрование данных → Шифрование съемных дисков.
5. В блоке Управление шифрованием выберите элемент Шифровать все файлы или элемент Шифровать только новые файлы.

   Портативный режим доступен только при шифрования файлов (FLE). Включить поддержку портативного режима для полнодискового шифрования (FDE) невозможно.
6. Установите флажок Портативный режим.
7. Если нужно, добавьте правила шифрования для отдельных съемных дисков.
8. Сохраните внесенные изменения.
9. После применения политики подключите съемный диск к компьютеру.
10. Подтвердите операцию шифрования съемного диска.

    Откроется окно создания пароля для портативного файлового менеджера.
11. Задайте пароль, соответствующий требованиям к уровню сложности, и подтвердите его.
12. Нажмите на кнопку OK.

    Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зашифрует файлы на съемном диске. Портативный файловый менеджер для работы с зашифрованными файлами будет также добавлен на съемный диск. Если на съемном диске уже есть зашифрованные файлы, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зашифрует их повторно с помощью собственного ключа. Это позволяет пользователю получить доступ ко всем файлам на съемном диске в портативном режиме.

Получение доступа к зашифрованным файлам на съемном диске

После шифрования файлов на съемном диске с поддержкой портативного режима доступны следующие способы доступа к файлам:

- Если на компьютере не установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, портативный файловый менеджер предложит ввести пароль. Пароль нужно будет вводить при каждой перезагрузке компьютера или переподключении съемного диска.
- Если компьютер находится за пределами корпоративной сети и на компьютере установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, программа предложит ввести пароль или отправить запрос на доступ к файлам администратору. После получения доступа к файлам на съемном диске Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохранит

секретный ключ в хранилище ключей компьютера. Это позволит в дальнейшем получить доступ к файлам без ввода пароля или запроса администратору.

- Если компьютер находится внутри корпоративной сети и на компьютере установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, вы получите доступ к устройству без ввода пароля. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready получит секретный ключ от Сервера администрирования Kaspersky Security Center к которому подключен компьютер.

Восстановление пароля для работы в портативном режиме

Если вы забыли пароль для работы в портативном режиме, вам нужно подключить съемный диск к компьютеру с установленной программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready внутри корпоративной сети. Вы получите доступ к файлам, так как в хранилище ключей компьютера или на Сервере администрирования сохранен секретный ключ. Расшифруйте и снова зашифруйте файлы с новым паролем.

Особенности работы портативного режима при подключении съемного диска к компьютеру из другой сети

Если компьютер находится за пределами корпоративной сети и на компьютере установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, вы можете получить доступ к файлам следующими способами:

- Доступ по паролю

  После ввода пароля вы сможете просматривать, изменять и сохранять файлы на съемном диске (прозрачный доступ). Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может установить для съемного диска право доступа "только чтение", если в параметрах политики для шифрования съемных дисков настроены следующие параметры:

  - Выключена поддержка портативного режима.
  - Выбран режим Шифровать все файлы или Шифровать только новые файлы.

  В остальных случаях вы получите полный доступ к съемному диску (право "чтение и запись"). Вам будет доступно добавление и удаление файлов.

  Вы можете изменить права доступа к съемному диску, даже если съемный диск подключен к компьютеру. Если права доступа к съемному диску изменились, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует доступ к файлам и запросит пароль повторно.

  После ввода пароля применить параметры политики шифрования для съемного диска невозможно. Таким образом, расшифровать или перешифровать файлы на съемном диске невозможно.

- Запрос доступа к файлам у администратора

  Если вы забыли пароль для работы в портативном режиме, запросите доступ к файлам у администратора. Для доступа к файлам пользователю нужно отправить файл запроса (файл с расширением kesdc) администратору. Пользователь можете отправить файл запроса, например, по электронной почте. Администратор отправит файл доступа к зашифрованным данным (файл с расширением kesdr).

  После прохождения процедуры восстановления пароля ("Запрос - Ответ") вы получите прозрачный доступ к файлам на съемном диске и полный доступ к съемному диску (право "запись и чтение").

Вы можете применить политику для шифрования съемных дисков и, например, расшифровать файлы. После восстановления пароля или при обновлении политики программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предложит подтвердить изменения.

Как получить файл доступа к зашифрованным данным в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Устройства.
4. На закладке Устройства выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт Предоставление доступа в офлайн-режиме.
6. В открывшемся окне выберите закладку Шифрование данных.
7. На закладке Шифрование данных нажмите на кнопку Обзор.
8. В окне выбора файла запроса укажите путь к файлу, полученного от пользователя.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.

Как получить файл доступа к зашифрованным данным в Web Console

1. В главном окне Web Console выберите Устройства → Управляемые устройства.
2. Установите флажок рядом с именем компьютера, доступ к данным которого вы хотите восстановить.
3. Нажмите на кнопку Предоставить доступ к устройству в автономном режиме.
4. Выберите раздел Шифрование данных.
5. Нажмите на кнопку Выбрать файл и выберите файл запроса, полученный от пользователя (файл с расширением kesdc).

Web Console покажет информацию о запросе. В том числе, имя компьютера, на котором пользователь запрашивает доступ к файлу.

6. Нажмите на кнопку Сохранить ключ и выберите папку для сохранения файла ключа доступа к зашифрованным данным (файл с расширением kesdr).

В результате вам будет доступен ключ доступа к зашифрованным данным, который нужно будет передать пользователю.

Расшифровка съемных дисков

Вы можете расшифровать съемный диск с помощью политики. Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы администрирования. Поэтому результат расшифровки данных на съемных дисках зависит от того, к какому компьютеру подключен съемный диск.

Чтобы расшифровать съемные диски, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Политики.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите Шифрование данных → Шифрование съемных дисков.
6. Если вы хотите расшифровать все зашифрованные файлы, хранящиеся на съемных дисках, в раскрывающемся списке Режим шифрования выберите действие Расшифровывать весь съемный диск.
7. Если вы хотите расшифровать данные, хранящиеся на отдельных съемных дисках, измените правила шифрования съемных дисков, данные которых вы хотите расшифровать. Для этого выполните следующие действия:
   a. В списке съемных дисков, для которых определены правила шифрования, выберите запись о нужном вам съемном диске.
   b. Нажмите на кнопку Задать правило, чтобы изменить правило шифрования для этого съемного диска.

      Откроется контекстное меню кнопки Задать правило.
   c. В контекстном меню кнопки Задать правило выберите пункт Расшифровывать все файлы.
8. Сохраните внесенные изменения.

В результате, если пользователь подключает съемный диск или он уже подключен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready расшифровывает съемный диск. Программа предупреждает пользователя, что процедура расшифровки может занять некоторое время. Если во время расшифровки данных пользователь инициирует безопасное извлечение съемного диска, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready прерывает расшифровку данных и позволяет извлечь съемный диск до завершения операции расшифровки. Расшифровка данных будет продолжена после следующего подключение съемного диска к компьютеру.

Если расшифровка съемного диска не удалась, просмотрите отчет Шифрование данных в интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Доступ к файлам может быть заблокирован другой программой. В этом случае попробуйте извлечь и заново подключить съемный диск к компьютеру.

Просмотр информации о шифровании данных

В процессе шифрования и расшифровки данных Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправляет на Kaspersky Security Center информацию о статусах применения параметров шифрования на клиентских компьютерах.

Возможны следующие статусы шифрования:

- Не задана политика шифрования. Для компьютера не назначена политика шифрования Kaspersky Security Center.
- В процессе применения политики. На компьютере выполняется шифрование и / или расшифровка данных.
- Ошибка. Во время шифрования и / или расшифровки данных на компьютере возникла ошибка.
- Требуется перезагрузка. Для инициализации или завершения шифрования или расшифровки данных на компьютере требуется перезагрузка операционной системы.
- Соответствует политике. Шифрование данных на компьютере выполнено в соответствии с параметрами шифрования, указанными в примененной к компьютеру политике Kaspersky Security Center.
- Отменено пользователем. Пользователь отказался подтвердить выполнение операции шифрования файлов на съемном диске.

Просмотр статусов шифрования

Чтобы просмотреть статус шифрования данных компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку Устройства.

   На закладке Устройства в рабочей области отображаются свойства компьютеров выбранной группы администрирования.
4. На закладке Устройства рабочей области сдвиньте полосу прокрутки до упора вправо.
5. Если графа Статус шифрования не отображается, выполните следующие действия:

   a. По правой клавиши мыши откройте контекстное меню для заголовочной части таблицы.

   b. В контекстном меню в выпадающем списке Вид выберите Добавить или удалить графы.

   Откроется окно Добавление или удаление граф.

   c. В окне Добавление или удаление граф установите флажок Статус шифрования. d. Нажмите на

   кнопку OK.

В графе Статус шифрования отображаются статусы шифрования данных для компьютеров выбранной группы администрирования. Этот статус формируется на основе информации о шифровании файлов на локальных дисках компьютера и полнодисковом шифровании.

Просмотр статистики шифрования на информационных панелях Kaspersky Security Center

Чтобы просмотреть статусы шифрования на информационных панелях Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите узел Сервер администрирования – <Имя компьютера>.
3. В рабочей области, расположенной справа от дерева Консоли администрирования, выберите закладку Статистика.
4. Создайте новую страницу с информационными панелями со статистикой шифрования данных. Для этого выполните следующие действия:
   a. На закладке Статистика нажмите на кнопку Настроить вид.

      Откроется окно Свойства: Статистика.

   b. В окне Свойства: Статистика нажмите на кнопку Добавить.

      Откроется окно Свойства: Новая страница.

   c. В разделе Общие окна Свойства: Новая страница введите название страницы.

   d. В разделе Информационные панели нажмите на кнопку Добавить.

      Откроется окно Новая информационная панель.

   e. В окне Новая информационная панель в группе Состояние защиты выберите элемент Шифрование устройств.

   f. Нажмите на кнопку OK.

      Откроется окно Свойства: Шифрование устройств.

   g. Измените при необходимости параметры информационной панели. Для этого воспользуйтесь разделами Вид и Устройства окна Свойства: Шифрование устройств.

   h. Нажмите на кнопку OK.

   i. Повторите пункты d – h инструкции, при этом в окне Новая информационная панель в группе Состояние защиты выберите элемент Шифрование съемных дисков.

      Добавленные информационные панели отобразятся в списке Информационные панели окна Свойства: Новая страница.

   j. В окне Свойства: Новая страница нажмите на кнопку OK.

      Название созданной на предыдущих шагах страницы с информационными панелями отобразится в списке Страницы окна Свойства: Статистика.

k. В окне Свойства: Статистика нажмите на кнопку Закрыть.

5. На закладке Статистика откройте страницу, созданную на предыдущих шагах инструкции.

Отобразятся информационные панели, на которых вы можете просмотреть статусы шифрования компьютеров и съемных дисков.

Просмотр ошибок шифрования файлов на локальных дисках компьютера

Чтобы просмотреть ошибки шифрования файлов на локальных дисках компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке Управляемые устройства дерева Консоли администрирования откройте папку с названием группы администрирования, где находится компьютер пользователя, для которого вы хотите просмотреть список ошибок шифрования файлов.
3. В рабочей области выберите закладку Устройства.
4. На закладке Устройства выделите в списке компьютер и по правой клавише мыши вызовите контекстное меню.
5. В контекстном меню компьютера выберите пункт Свойства. В открывшемся окне Свойства: <название компьютера> выберите раздел Защита.
6. В разделе Защита окна Свойства: <название компьютера> по ссылке Просмотреть ошибки шифрования данных откройте окно Ошибки шифрования данных.

В этом окне отображается информация об ошибках шифрования файлов на локальных дисках компьютера. Если ошибка исправлена, то Kaspersky Security Center удаляет информацию о ней из окна Ошибки шифрования данных.

Просмотр отчета о шифровании данных

Чтобы просмотреть отчет о шифровании данных, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле Сервер администрирования дерева Консоли администрирования выберите закладку Отчеты.
3. Нажмите на кнопку Новый шаблон отчета.

   Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. В окне Выбор типа шаблона отчета в разделе Другое выберите один из следующих пунктов:

- Отчет о статусе шифрования управляемых устройств.
- Отчет о статусе шифрования запоминающих устройств.
- Отчет об ошибках шифрования файлов.
- Отчет о блокировании доступа к зашифрованным файлам.

После завершения работы мастера создания шаблона отчета в таблице на закладке Отчеты появится новый шаблон отчета.

5. Выберите шаблон отчета, созданный на предыдущих шагах инструкции.
6. В контекстном меню шаблона выберите пункт Показать отчет.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Работа с зашифрованными устройствами при отсутствии доступа к ним

Получение доступа к зашифрованным устройствам

Пользователю может потребоваться запросить доступ к зашифрованным устройствам в следующих случаях:

- Жесткий диск был зашифрован на другом компьютере.
- На компьютере нет ключа шифрования для устройства (например, в момент первого обращения к зашифрованному съемному диску на этом компьютере), и связь с Kaspersky Security Center отсутствует.

После того как пользователь применил ключ доступа к зашифрованному устройству, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет ключ шифрования на компьютере пользователя и предоставляет доступ к этому устройству при последующих обращениях, даже если связь с Kaspersky Security Center отсутствует.

Получение доступа к зашифрованным устройствам осуществляется следующим образом:

1. Пользователь создает через интерфейс программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready файл запроса доступа с расширением kesdc и передает его администратору локальной сети организации.
2. Администратор создает в Консоли администрирования Kaspersky Security Center файл ключа доступа с расширением kesdr и передает его пользователю.
3. Пользователь применяет ключ доступа.

Восстановление данных на зашифрованных устройствах

Для работы с зашифрованными устройствами пользователь может использовать утилиту восстановления зашифрованных устройств (далее – "утилита восстановления"). Это может потребоваться в следующих случаях:

- Процедура получения доступа с помощью ключа доступа прошла неуспешно.
- На компьютере с зашифрованным устройством не установлены компоненты шифрования.

Данные, необходимые для восстановления доступа к зашифрованным устройствам с помощью утилиты восстановления, в течение некоторого времени находятся в памяти компьютера пользователя в открытом виде. Чтобы снизить вероятность несанкционированного доступа к этим данным, рекомендуется выполнять восстановление доступа к зашифрованным устройствам на доверенных компьютерах.

Восстановление данных на зашифрованных устройствах осуществляется следующим способом:

1. Пользователь создает с помощью утилиты восстановления файл запроса доступа с расширением fdertc и передает его администратору локальной сети организации.
2. Администратор создает в Консоли администрирования Kaspersky Security Center файл ключа доступа с расширением fdertr и передает его пользователю.
3. Пользователь применяет ключ доступа.

Для восстановления данных на зашифрованных системных жестких дисках пользователь также может указать в утилите восстановления учетные данные Агента аутентификации. Если метаданные учетной записи Агента аутентификации повреждены, то пользователю потребуется пройти процедуру восстановления с помощью файла запроса доступа.

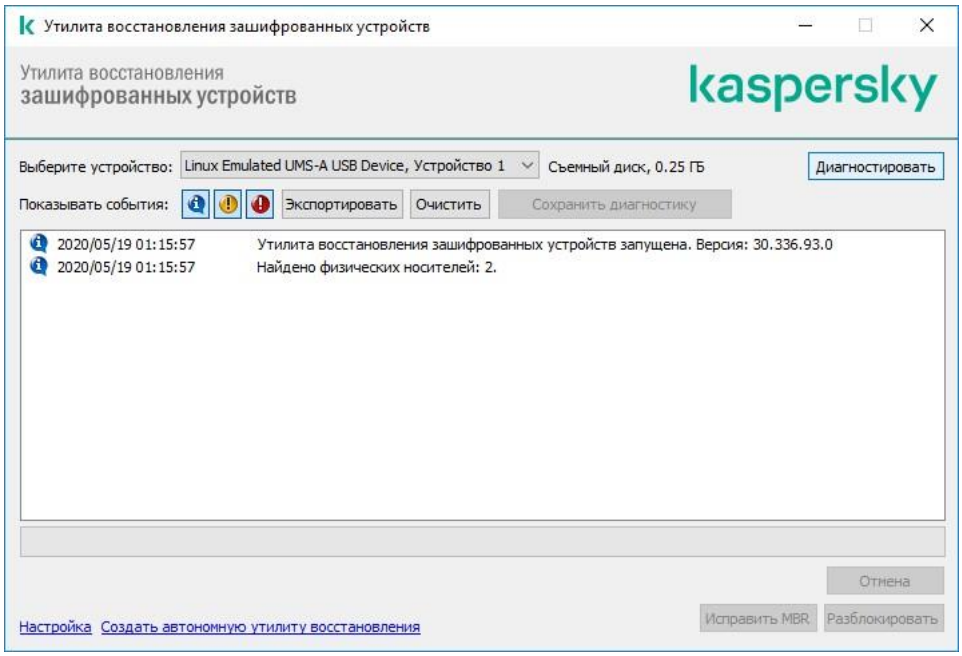
Перед восстановлением данных на зашифрованных устройствах рекомендуется вывести компьютер, на котором будет выполняться процедура, из-под действия политики Kaspersky Security Center или отключить шифрование в параметрах политики Kaspersky Security Center. Это позволяет предотвратить повторное шифрование устройства.

Восстановление данных с помощью утилиты восстановления FDERT

При неисправности жесткого диска файловая система может быть повреждена. Таким образом, данные, защищенные технологией Шифрование диска Kaspersky, будут недоступны. Вы можете расшифровать данные и скопировать данные на новый диск.

Восстановление данных на диске, защищенные технологией Шифрование диска Kaspersky, состоит из следующих этапов:

1. Создание автономной утилиты восстановления (см. рис. ниже).
2. Подключение диска к компьютеру, на котором отсутствуют компоненты шифрования Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.
3. Запуск утилиты восстановления и диагностика жесткого диска.
4. Доступ к данным на диске. Для этого нужно ввести учетные данные Агента аутентификации или запустить процедуру восстановления ("Запрос - Ответ").



Утилита восстановления FDERT

Создание автономной утилиты восстановления

Чтобы создать исполняемый файл утилиты восстановления, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Поддержка.
2. В открывшемся окне нажмите на кнопку Восстановление зашифрованного устройства.

   Запустится утилита восстановления зашифрованных устройств.
3. В окне утилиты восстановления нажмите на кнопку Создать автономную утилиту восстановления.
4. Сохраните автономную утилиту восстановления в память компьютера.

В результате исполняемый файл утилиты восстановления fdert.exe будет сохранен в указанной папке. Скопируйте утилиту восстановления на компьютер, на котором отсутствуют компоненты шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Это позволяет предотвратить повторное шифрование диска.

Данные, необходимые для восстановления доступа к зашифрованным устройствам с помощью утилиты восстановления, в течение некоторого времени находятся в памяти компьютера пользователя в открытом виде. Чтобы снизить вероятность несанкционированного доступа к этим данным, рекомендуется выполнять восстановление доступа к зашифрованным устройствам на доверенных компьютерах.

Восстановление данных на жестком диске

Чтобы восстановить доступ к зашифрованному устройству с помощью утилиты восстановления, выполните следующие действия:

1. Запустите исполняемый файл утилиты восстановления fdert.exe, созданный с помощью программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

2. В окне утилиты восстановления в раскрывающемся списке Выберите устройство выберите зашифрованное устройство, доступ к которому вы хотите восстановить.

3. Нажмите на кнопку Диагностировать, чтобы утилита могла определить, какое действие следует выполнить с зашифрованным устройством: разблокировать или расшифровать.

   Если на компьютере доступна функциональность шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, то утилита восстановления предлагает разблокировать устройство. При разблокировке устройство не расшифровывается, но к нему в результате предоставляется прямой доступ. Если на компьютере недоступна функциональность шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, то утилита восстановления предлагает расшифровать устройство.

4. Если вы хотите импортировать диагностическую информацию, нажмите на кнопку Сохранить диагностику.

   Утилита сохранит архив с файлами с диагностической информацией.

5. Нажмите на кнопку Исправить MBR, если в результате диагностики зашифрованного системного жесткого диска вы получили сообщение о каких-либо проблемах, связанных с главной загрузочной записью (MBR) устройства.

   Исправление главной загрузочной записи устройства может ускорить получение информации, необходимой для разблокировки или расшифровки устройства.

6. Нажмите на кнопку Разблокировать или Расшифровать в зависимости от результатов диагностики.

7. Если вы хотите восстановить данные с помощью учетной записи Агента аутентификации, выберите вариант Использовать параметры учетной записи Агента аутентификации и введите учетные данные Агента аутентификации.

   Этот способ возможен только при восстановлении данных на системном жестком диске. Если системный жесткий диск был поврежден и данные об учетной записи Агента аутентификации потеряны, то для восстановления данных на зашифрованном устройстве необходимо получить ключ доступа у администратора локальной сети организации.

8. Если вы хотите запустить процедуру восстановления, выполните следующие действия:

   a. Выберите вариант Указать ключ доступа к устройству вручную.

   b. Нажмите на кнопку Получить ключ доступа и сохраните файл запроса в память компьютера (файл с расширением fdertc).

   c. Передайте файл запроса доступа администратору локальной сети организации.

      Не закрывайте окно Получение ключа доступа к устройству, пока вы не получите ключ доступа. При повторном открытии этого окна созданный администратором ранее ключ доступа будет невозможно применить.

   d. Получите и сохраните файл доступа (файл с расширением fdertr), созданный и переданный вам администратором локальной сети организации (см. инструкцию ниже).

   e. Загрузите файл доступа в окне Получение ключа доступа к устройству.

9. Если вы выполняете расшифровку устройства, требуется настроить дополнительные параметры расшифровки:

   - Укажите область для расшифровки:

     - Если вы хотите расшифровать все устройство, выберите вариант Расшифровать все устройство.
     - Если вы хотите расшифровать часть данных на устройстве, выберите вариант Расшифровать отдельные области устройства и задайте границы области для расшифровки.

   - Выберите место записи расшифрованных данных:

     - Если вы хотите, чтобы данные на исходном устройстве были перезаписаны расшифрованными данными, снимите флажок Расшифровка в файл образа диска.
     - Если вы хотите сохранить расшифрованные данные отдельно от исходных зашифрованных данных, установите флажок Расшифровка в файл образа диска и с помощью кнопки Обзор укажите путь, по которому файл формата VHD должен быть сохранен.

10. Нажмите на кнопку OK.

Запустится процесс разблокировки / расшифровки устройства.

Как создать файл доступа к зашифрованным данным в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве Консоли администрирования выберите папку Дополнительно → Шифрование и защита данных → Зашифрованные устройства.

3. В рабочей области выберите зашифрованное устройство, для которого вы хотите создать файл ключа доступа, и в контекстном меню устройства выберите пункт Получить доступ к устройству в Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).

   Если вы не уверены, для какого компьютера был сформирован файл запроса доступа, в дереве Консоли администрирования выберите папку Дополнительно → Шифрование и защита данных и в рабочей области нажмите на ссылку Получить ключ шифрования устройства в Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows (11.4.0).

4. В открывшемся окне выберите используемый алгоритм шифрования: AES256 или AES56.

   Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: Strong encryption (AES256) или Lite encryption (AES56). Библиотека шифрования AES устанавливается вместе с программой.

5. Нажмите на кнопку Обзор и в открывшемся окне укажите путь к файлу запроса, полученного от пользователя, с расширением fdertc.

6. Нажмите на кнопку Открыть.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.

Как создать файл доступа к зашифрованным данным в Web Console

1. В главном окне Web Control выберите Операции → Шифрование и защита данных → Зашифрованные устройства.

2. Установите флажок рядом с именем компьютера, данные на котором вы хотите восстановить.

3. Нажмите на кнопку Предоставить доступ к устройству в автономном режиме.

   Запустится мастер предоставления доступа к устройству.

4. Следуйте указаниям мастера предоставления доступа к устройству:

   a. Выберите плагин Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для Windows.

   b. Выберите используемый алгоритм шифрования: AES256 или AES56.

      Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: Strong encryption (AES256) или Lite encryption (AES56). Библиотека шифрования AES устанавливается вместе с программой.

   c. Нажмите на кнопку Выбрать файл и выберите файл запроса, полученного от пользователя (файл с расширением fdertc).

   d. Нажмите на кнопку Сохранить ключ и выберите папку для сохранения файла ключа доступа к зашифрованным данным (файл с расширением fdertr).

В результате вам будет доступен ключ доступа к зашифрованным данным, который нужно будет передать пользователю.

Создание диска аварийного восстановления операционной системы

Диск аварийного восстановления операционной системы может быть полезен в ситуации, когда по какимлибо причинам доступ к зашифрованному системному жесткому диску невозможен и операционная система не может быть загружена.

Вы можете загрузить образ операционной системы Windows с помощью диска аварийного восстановления и восстановить доступ к зашифрованному системному диску с помощью утилиты восстановления, включенной в состав образа операционной системы.

Чтобы создать диск аварийного восстановления операционной системы, выполните следующие действия:

1. Создайте исполняемый файл утилиты восстановления зашифрованных устройств.

2. Создайте пользовательский образ среды предустановки Windows. В процессе создания пользовательского образа среды предустановки Windows добавьте в образ исполняемый файл утилиты восстановления зашифрованных устройств.

3. Поместите пользовательский образ среды предустановки Windows на загрузочный носитель, например компакт-диск или съемный диск.

   Инструкцию о создании пользовательского образа среды предустановки Windows вы можете прочитать в справочной документации Microsoft (например, на ресурсе Microsoft TechNet).

Управление программой из командной строки

Вы можете управлять Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из командной строки. Вы можете просмотреть список команд для управления программой с помощью команды `HELP`. Чтобы получить справку по синтаксису конкретной команды, введите `HELP <команда>`.

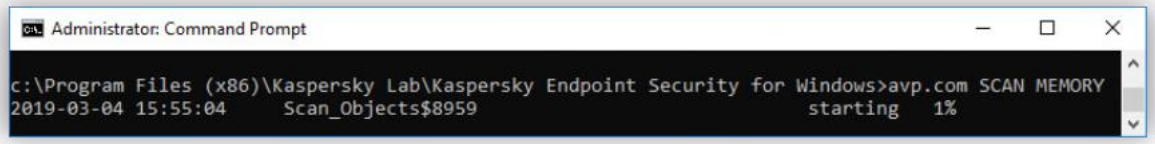
Команды

Чтобы управлять Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из командной строки, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
3. Используйте следующий шаблон для выполнения команды:

```
avp.com <команда> [параметры]
```

В результате Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполнит команду (см. рис. ниже).



Управление программой из командной строки

SCAN. Антивирусная проверка

Запустить задачу антивирусной проверки.

Синтаксис команды

```
SCAN [<область проверки>] [<действие при обнаружении угрозы>] [<типы файлов>]
[<исключения из проверки>] [/R[A]:<файл отчета>] [<технологии проверки>] [/C:<файл с
параметрами антивирусной проверки>]
```

Область проверки	

<файлы для проверки>	Список файлов и папок через пробел. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например: • `"C:\Program Files (x86)\Example Folder"` – длинный путь. • `C:\PROGRA~2\EXAMPL~1` – короткий путь.
/ALL	Запустить задачу Полная проверка. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет следующие объекты: • память ядра; объекты, загрузка которых осуществляется при запуске операционной системы; загрузочные секторы; резервное хранилище • операционной системы; все жесткие и съемные диски. • • •
/MEMORY	Проверить память ядра.
/STARTUP	Проверить объекты, загрузка которых осуществляется при запуске операционной системы.
/MAIL	Проверить почтовый ящик Outlook.
/REMDRIVES	Проверить съемные диски.
/FIXDRIVES	Проверить жесткие диски.
/NETDRIVES	Проверить сетевые диски.
/QUARANTINE	Проверить файлы в резервном хранилище Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
/@:<список файлов.lst>	Проверить файлы и папки, перечисленные в списке. Каждый файл из списка нужно вводить с новой строки. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например: • `"C:\Program Files (x86)\Example Folder"` – длинный путь. • `C:\PROGRA~2\EXAMPL~1` – короткий путь.
Действие при обнаружении угрозы	

/i0	Информировать. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавляет информацию об этих файлах в список активных угроз.
/i1	Лечить; информировать, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавляет информацию об обнаруженных зараженных файлах в список активных угроз.
/i2	Лечить; удалять, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready их удаляет. Этот вариант действия выбран по умолчанию.
/i3	Лечить обнаруженные зараженные файлы. Если лечение невозможно, удалять зараженные файлы. Также удалять составные файлы (например, архивы), если вылечить или удалить зараженный файл невозможно.

/i4	Удалять зараженные файлы. Также удалять составные файлы (например, архивы), если удалить зараженный файл невозможно.
/i8	Запрашивать действие у пользователя сразу после обнаружения угрозы.
/i9	Запрашивать действие у пользователя после выполнения проверки.
Типы файлов	
/fe	Файлы, проверяемые по расширению. Если выбран этот параметр, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
/fi	Файлы, проверяемые по формату. Если выбран этот параметр, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.
/fa	Все файлы. Если выбран этот параметр, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет все файлы без исключения (любых форматов и расширений). Параметр выбран по умолчанию.
Исключения из проверки	
-e:a	Исключение из проверки архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
-e:b	Исключение из проверки почтовых баз, входящих и исходящих сообщений электронной почты.

`-e:<маска файла>`	Исключение из проверки файлов по маске. Например: • Маска `*.exe` будет включать все пути к файлам с расширением exe. • Маска `example*` будет включать все пути к файлам с именем EXAMPLE.
`-e:<секунды>`	Исключение из проверки файлов, длительность проверки которых превышает установленное значение в секундах.
`-es:<мегабайты>`	Исключение из проверки файлов, размер которых превышает установленное значение в мегабайтах.
Режим сохранения событий в файл отчета	
`/R:<файл отчета>`	Сохранять только критические события в файл отчета.
`/RA:<файл отчета>`	Сохранять все события в файл отчета.
Технологии проверки	
`/iChecker=on|off`	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, дату предыдущей проверки файла, а также изменение параметров проверки.
`/iSwift=on|off`	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
Дополнительные параметры	
`/C:<файл с параметрами антивирусной проверки>`	Файл с параметрами задачи антивирусной проверки. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: `[<область проверки>] [<действие при обнаружении угрозы>] [<типы файлов>] [<исключения из проверки>] [/R[A]:<файл отчета>] [<технологии проверки>]`.

Пример:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Обновление баз и модулей программы

Запустить задачу Обновление.

```
Синтаксис команды
```

```
UPDATE ["<источник обновления>"] [/R[A]:<файл отчета>] [/C:<файл с параметрами обновления>]
```

Источник обновления	
"<источник обновления>"	Адрес HTTP-, FTP-сервера или папки общего доступа с пакетом обновлений. Вы можете указать только один источник обновления. Если источник обновлений не указан, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует источник, указанный в задаче Обновление. Задача Обновление создается автоматически после установки программы.

Режим сохранения событий в файл отчета	
/R:<файл отчета>	Сохранять только критические события в файл отчета.
/RA:<файл отчета>	Сохранять все события в файл отчета.

Дополнительные параметры	
/C:<файл с параметрами обновления>	Файл с параметрами задачи Обновление. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: ["<источник обновления>"] [/R[A]:<файл отчета>].

Пример:
```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Откат последнего обновления

Откатить последние обновления антивирусных баз. Это позволяет вернуться к использованию предыдущей версии баз и модулей программы при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует безопасную программу.

Синтаксис команды

```
ROLLBACK [/R[A]:<файл отчета>]
```

Режим сохранения событий в файл отчета	
/R:<файл отчета>	Сохранять только критические события в файл отчета.
/RA:<файл отчета>	Сохранять все события в файл отчета.

Пример: `avp.com ROLLBACK /RA:rollback.txt`

TRACES. Трассировка

Включить / выключить трассировку. Файлы трассировки хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. По умолчанию трассировка выключена.

Синтаксис команды

```
TRACES on|off [<уровень трассировки>] [<дополнительные параметры>]
```

Уровень трассировки	
<уровень трассировки>	Уровень детализации трассировки. Возможные значения: • 100 (критический). Только сообщения о неустранимых ошибках. • 200 (высокий). Сообщения о всех ошибках, включая неустранимые. • 300 (диагностический). Сообщения о всех ошибках, а также предупреждения. • 400 (важный). Сообщения о всех ошибках, предупреждения, а также дополнительная информация. • 500 (обычный). Сообщения о всех ошибках, предупреждениях, а также подробная информация о работе программы в нормальном режиме (значение по умолчанию). • 600 (низкий). Все сообщения.

Дополнительные параметры	
all	Выполнить команду с параметрами dbg, file и mem.
dbg	Использовать функцию OutputDebugString и сохранять файл трассировки. Функция OutputDebugString отправляет символьную строку отладчику программы для вывода на экран. Подробнее см. на сайте MSDN.
file	Сохранить один файл трассировки (без ограничений по размеру).
rot	Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера.
mem	Записывать результаты трассировки в файлы дампов.

Примеры: avp.com TRACES on 500

- avp.com TRACES on 500 dbg
  avp.com TRACES off avp.com
- TRACES on 500 dbg mem
  avp.com TRACES off file
-
-
-

START. Запуск профиля

Запустить выполнение профиля (например, запустить обновление баз или включить компонент защиты).

Синтаксис команды

```
START <профиль> [/R[A]:<файл отчета>]
```

Профиль	
<профиль>	Название профиля. Профиль – компонент, задача или функция Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Список доступных профилей вы можете узнать по команде HELP START.

Режим сохранения событий в файл отчета	
/R:<файл отчета>	Сохранять только критические события в файл отчета.
/RA:<файл отчета>	Сохранять все события в файл отчета.

Пример:
avp.com START Scan_Objects

STOP. Остановка профиля

Остановить выполняемый профиль (например, остановить проверку съемных дисков или выключить компонент защиты).

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешения Выключение компонентов защиты, Выключение компонентов контроля.

Синтаксис команды

```
STOP <профиль> /login=<имя пользователя> /password=<пароль>
```

Профиль	

<профиль>	Название профиля. Профиль – компонент, задача или функция Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Список доступных профилей вы можете узнать по команде HELP STOP.
Авторизация	
/login=<имя пользователя> /password=<пароль>	Данные учетной записи пользователя с необходимыми разрешениями Защиты паролем.

STATUS. Статус профиля

Показать информацию о состоянии профилей программы (например, running или completed). Список доступных профилей вы можете узнать по команде HELP STATUS.

Также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready показывает информацию о состоянии служебных профилей. Информация о состоянии служебных профилей может понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

Синтаксис команды

```
STATUS [<профиль>]
```

STATISTICS. Статистика выполнения профиля

Показать статистическую информацию о профиле программы (например, время проверки или количество обнаруженных угроз). Список доступных профилей вы можете узнать по команде HELP STATISTICS.

Синтаксис команды

```
STATISTICS <профиль>
```

RESTORE. Восстановление файлов

Восстановить файл из резервного хранилища в папку его исходного размещения. Если по указанному пути уже существует файл с таким же именем, к имени файла добавляется суффикс "-copy". Восстанавливаемый файл копируется с исходным именем.

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение Восстановление из резервного хранилища.

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. Резервная копия – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке C:\ProgramData\Kaspersky Lab\KES\QB.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

В Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Синтаксис команды

```
RESTORE [/REPLACE] <имя файла> /login=<имя пользователя> /password=<пароль>
```

Дополнительные параметры	
/REPLACE	Переписать существующий файл.
<имя файла>	Имя восстанавливаемого файла.

Авторизация	
/login=<имя пользователя> /password=<пароль>	Данные учетной записи пользователя с необходимыми разрешениями Защиты паролем.

Пример: `avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1`

EXPORT. Экспорт параметров программы

Экспортировать параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в файл. Файл будет размещен в папке C:\Windows\SysWOW64.

Синтаксис команды

```
EXPORT <профиль> <имя файла>
```

Профиль	
<профиль>	Название профиля. Профиль – компонент, задача или функция Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Список доступных профилей вы можете узнать по команде `HELP EXPORT`.

Файл для экспорта	
<имя файла>	Имя файла, в который должны быть экспортированы параметры профиля. Вы можете экспортировать параметры профиля в конфигурационный файл в формате DAT или CFG, в текстовый файл в формате TXT или в документ в формате XML.

Примеры: `avp.com EXPORT ids`

- `ids_config.dat avp.com EXPORT fm fm_config.txt`
-

IMPORT. Импорт параметров программы

Импортировать параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из файла, который был создан с помощью команды `EXPORT`.

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение Настройка параметров программы.

Синтаксис команды

```
IMPORT <имя файла> /login=<имя пользователя> /password=<пароль>
```

Файл для импорта	
`<имя файла>`	Имя файла, из которого должны быть импортированы параметры программы. Вы можете импортировать параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из конфигурационного файла в формате DAT или CFG, текстового файла в формате TXT или документа в формате XML.

Авторизация	
`/login=<имя пользователя> /password=<пароль>`	Данные учетной записи пользователя с необходимыми разрешениями Защиты паролем.

Пример:
`avp.com IMPORT config.dat /login=KLAdmin /password=!Password1`

ADDKEY. Применение файла ключа

Применить файл ключа для активации Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если программа уже активирована, ключ будет добавлен в качестве резервного.

Синтаксис команды

```
ADDKEY <имя файла> [/login=<имя пользователя> /password=<пароль>]
```

Файл ключа	
`<имя файла>`	Имя файла ключа.

Авторизация	
`/login=<имя пользователя> /password=<пароль>`	Данные учетной записи пользователя. Данные учетные записи нужно вводить, только если включена Защита паролем.

Пример: `avp.com ADDKEY file.key`

LICENSE. Лицензирование

Выполнить операции с лицензионными ключами программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Для выполнения команды удаления лицензионного ключа должна быть включена Защита паролем. Пользователь должен иметь разрешение Удаление ключа.

Синтаксис команды

```
LICENSE <операция> [/login=<имя пользователя> /password=<пароль>]
```

Операция	
/ADD <имя файла>	Применить файл ключа для активации Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Если программа уже активирована, ключ будет добавлен в качестве резервного.
/ADD <код активации>	Активировать Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с помощью кода активации. Если программа уже активирована, ключ будет добавлен в качестве резервного.
/REFRESH <имя файла>	Продлить срок действия лицензии с помощью файла ключа. В результате будет добавлен резервный ключ, который станет активным по истечении срока действия лицензии. Добавить активный ключ с помощью этой команды невозможно.
/REFRESH <код активации>	Продлить срок действия лицензии с помощью кода активации. В результате будет добавлен резервный ключ, который станет активным по истечении срока действия лицензии. Добавить активный ключ с помощью этой команды невозможно.
/DEL /login= <имя пользователя> /password= <пароль>	Удалить лицензионный ключ. Также будет удален резервный ключ.

Авторизация	
/login=<имя пользователя> /password=<пароль>	Данные учетной записи пользователя с необходимыми разрешениями Защиты паролем.

Пример: avp.com LICENSE /ADD file.key avp.com LICENSE /ADD

- AAAAA-BBBBB-CCCCC-DDDDD avp.com LICENSE /DEL /login=KLAdmin /password=!Password1
-
-

RENEW. Покупка лицензии

Перейти на веб-сайт "Лаборатории Касперского" для покупки лицензии или продления ее срока действия.

PBATESTRESET. Сбросить результаты проверки перед шифрованием диска

Сбросить результаты проверки поддержки полнодискового шифрования (FDE) по технологиям Шифрование диска Kaspersky и BitLocker.

Перед запуском полнодискового шифрования программа выполняет ряд проверок на возможность шифрования компьютера. Если полнодисковое шифрование невозможно, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет информацию о несовместимости. При следующей попытке шифрования программа не выполняет проверки и предупреждает о том, что шифрование невозможно. Если аппаратная конфигурация компьютера изменилась, то для проверки системного жесткого диска на совместимость с технологией Шифрования диска Kaspersky или BitLocker требуется сбросить информацию о несовместимости, полученную программой при предыдущей проверке.

EXIT. Завершение работы программы

Завершить работу Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Программа будет выгружена из оперативной памяти компьютера.

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение Завершение работы программы.

Синтаксис команды

```
EXIT /login=<имя пользователя> /password=<пароль>
```

EXITPOLICY. Выключение политики

Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (🔒).

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение Выключение политики Kaspersky Security Center.

Синтаксис команды

```
EXITPOLICY /login=<имя пользователя> /password=<пароль>
```

STARTPOLICY. Включение политики

Включить политику Kaspersky Security Center на компьютере. Параметры программы будут настроены в соответствии с политикой.

DISABLE. Выключение защиты

Выключить Защиту от файловых угроз на компьютере с истекшей лицензией на Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Выполнить команду на компьютере с неактивированной программой или с действующей лицензией невозможно.

SPYWARE. Обнаружение шпионского ПО

Включить / выключить обнаружение шпионского ПО. По умолчанию обнаружение шпионского ПО включено.

Синтаксис команды

```
SPYWARE on|off
```

Коды ошибок

При работе с программой через командную строку возможно появление ошибок. При появлении ошибки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready показывает сообщение об ошибке, например, `Error: Cannot start task 'EntAppControl'`. Также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может показать дополнительные сведения в виде кода, например, `error=8947906D` (см. таблицу ниже).

Коды ошибок

Код ошибки	Описание
09479001	Лицензионный ключ для Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready уже используется на этом компьютере.
0947901D	Срок действия лицензии истек. Обновление баз недоступно.
89479002	Ключ не найден.
89479003	Цифровая подпись повреждена или не найдена.
89479004	Данные повреждены.
89479005	Файл ключа поврежден.
89479006	Истек срок действия лицензии или срок годности лицензионного ключа.
89479007	Файл ключа не указан.
89479008	Невозможно применить файл ключа.
89479009	Не удалось сохранить данные.
8947900A	Не удалось прочитать данные.
8947900B	Ошибка ввода/вывода.

8947900C	Базы не найдены.
8947900E	Библиотека лицензирования не загружена.
8947900F	Базы повреждены или обновлены вручную.
89479010	Базы повреждены.
89479011	Невозможно применить недействительный файл ключа для добавления резервного ключа.
89479012	Системная ошибка.
89479013	Черный список ключей поврежден.
89479014	Цифровая подпись файла не соответствует цифровой подписи "Лаборатории Касперского".
89479015	Невозможно использовать ключ для некоммерческой лицензии в качестве ключа для коммерческой лицензии.
89479016	Чтобы использовать бета-версию программы, требуется лицензия на бета-тестирование.
89479017	Файл ключа не подходит для данной программы.
89479018	Ключ заблокирован "Лабораторией Касперского".
89479019	Программа уже использовалась по пробной лицензии. Невозможно снова добавить ключ для пробной лицензии.
8947901A	Файл ключа поврежден.
8947901B	Цифровая подпись не найдена, повреждена или не соответствует цифровой подписи "Лаборатории Касперского".
8947901C	Невозможно добавить ключ, если срок действия соответствующей ему некоммерческой лицензии истек.
8947901E	Дата создания файла ключа или его применения некорректна. Проверьте системную дату.
8947901F	Невозможно добавить ключ для пробной лицензии, пока действует другая аналогичная лицензия.
89479020	Черный список ключей поврежден или не найден.
89479021	Описание обновлений повреждено или не найдено.
89479022	Ошибка в служебных данных о лицензионном ключе.
89479023	Невозможно применить недействительный файл ключа для добавления резервного ключа.

89479025	Ошибка при отправке запроса на сервер активации. Возможные причины: ошибка соединения с интернетом или временные проблемы на сервере активации. Попробуйте активировать программу с помощью кода активации позже. В случае повторения ошибки обратитесь к вашему интернет-провайдеру.
89479026	Ошибка в ответе от сервера активации.
89479027	Невозможно получить статус ответа.
89479028	Ошибка при сохранении временного файла.
89479029	Введен неверный код активации или на компьютере установлена некорректная системная дата. Проверьте системную дату на компьютере.
8947902A	Файл ключа не подходит для данной программы или истек срок действия лицензии. Невозможно активировать Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с помощью файла ключа для другой программы.
8947902B	Не удалось получить файл ключа. Введен неверный код активации.
8947902C	Сервер активации возвратил ошибку 400.
8947902D	Сервер активации возвратил ошибку 401.
8947902E	Сервер активации возвратил ошибку 403.
8947902F	Сервер активации возвратил ошибку 404.
89479030	Сервер активации возвратил ошибку 405.
89479031	Сервер активации возвратил ошибку 406.
89479032	Требуется аутентификация на прокси-сервере. Проверьте параметры сети.
89479033	Время ожидания запроса истекло.
89479034	Сервер активации возвратил ошибку 409.
89479035	Сервер активации возвратил ошибку 410.
89479036	Сервер активации возвратил ошибку 411.
89479037	Сервер активации возвратил ошибку 412.
89479038	Сервер активации возвратил ошибку 413.
89479039	Сервер активации возвратил ошибку 414.
8947903A	Сервер активации возвратил ошибку 415.
8947903C	Внутренняя ошибка сервера.
8947903D	Функциональность не поддерживается.
8947903E	Некорректный ответ от шлюза. Проверьте параметры сети.
8947903F	Служба недоступна (ошибка HTTP 503).
89479040	Время ожидания ответа от шлюза истекло. Проверьте параметры сети.

89479041	Протокол не поддерживается сервером.
89479043	Неизвестная ошибка HTTP.

89479044	Некорректный идентификатор ресурса.
89479046	Некорректный адрес (URL).
89479047	Некорректная целевая папка.
89479048	Ошибка выделения памяти.
89479049	Ошибка конвертации параметров в ANSI-строку (url, folder, agent).
8947904A	Ошибка создания рабочего потока.
8947904B	Рабочий поток уже запущен.
8947904C	Рабочий поток не запущен.
8947904D	Файл ключа не найден на сервере активации.
8947904E	Ключ заблокирован.
8947904F	Внутренняя ошибка сервера активации.
89479050	Недостаточно данных в запросе на активацию.
89479053	Срок годности лицензионного ключа истек.
89479054	На компьютере установлена некорректная системная дата.
89479055	Срок действия пробной лицензии истек.
89479056	Истек срок действия лицензии.
89479057	Превышено допустимое количество активаций программы с помощью указанного кода.
89479058	Процедура активации завершилась с системной ошибкой.
89479059	Невозможно использовать ключ для некоммерческой лицензии в качестве ключа для коммерческой лицензии.
8947905C	Требуется код активации.
89479062	Невозможно подключиться к серверу активации.
89479064	Сервер активации недоступен. Проверьте параметры подключения к интернету и попробуйте активировать программу снова.
89479065	Дата выпуска баз программы превышает дату окончания срока действия лицензии.
89479066	Невозможно заменить активный ключ на ключ с истекшим сроком годности.
89479067	Невозможно добавить резервный ключ, если его срок годности истекает раньше по сравнению с действующей лицензией.

89479068	Отсутствует обновленный ключ по подписке.
8947906A	Неверный код активации (не совпадает контрольная сумма).
8947906B	Ключ уже активен.
8947906C	Типы лицензий, которые соответствуют активному и резервному ключам, не совпадают.
8947906D	Лицензия не допускает работу компонента.
8947906E	Невозможно добавить ключ по подписке в качестве резервного.
89479213	Общая ошибка транспортного уровня.
89479214	Не удалось связаться с сервером активации.
89479215	Неверный формат веб-адреса.

89479216	Не удалось преобразовать адрес прокси-сервера.
89479217	Не удалось преобразовать адрес сервера. Проверьте параметры подключения к интернету.
89479218	Не удалось связаться с сервером активации или с прокси-сервером.
89479219	Отказ в удалённом доступе.
8947921A	Время ожидания ответа истекло.
8947921B	Ошибка отправки HTTP-запроса.
8947921C	Ошибка SSL-соединения.
8947921D	Операция прервана в результате обратного вызова.
8947921E	Слишком много перенаправлений.
8947921F	Проверка адресата завершилась с ошибкой.
89479220	Пустой ответ от сервера активации.
89479221	Ошибка отправки данных.
89479222	Ошибка приема данных.
89479223	Ошибка локального SSL-сертификата.
89479224	Ошибка SSL-шифрования.
89479225	Ошибка SSL-сертификата сервера.
89479226	Некорректное содержимое сетевого пакета.
89479227	Пользователю отказано в доступе.
89479228	Некорректный файл SSL-сертификата.

89479229	Не удалось установить SSL-соединение.
8947922A	Не удалось отправить или принять сетевой пакет. Повторите попытку позднее.
8947922B	Некорректный файл с отозванными сертификатами.
8947922C	Ошибка запроса SSL-сертификата.
89479401	Неизвестная ошибка сервера.
89479402	Внутренняя ошибка сервера.
89479403	Лицензионный ключ для введенного кода активации отсутствует.
89479404	Активный ключ заблокирован.
89479405	Отсутствуют обязательные параметры запроса для активации программы.
89479406	Неверные имя пользователя или пароль.
89479407	На сервер передан неверный код активации.
89479408	Код активации не подходит для Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Неизвестно, для какой программы предназначен код активации.
89479409	В запросе отсутствует код активации.
8947940B	Истек срок действия лицензии (по данным от сервера активации).
8947940C	Превышено число активаций программы с помощью этого кода активации.
8947940D	Неверный формат идентификатора запроса.
8947940E	Код активации не подходит для Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Код активации предназначен для другой программы "Лаборатории Касперского".
8947940F	Невозможно обновить лицензионный ключ.
89479410	Код активации не подходит для этого региона.
89479411	Код активации не подходит для языковой версии Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.
89479412	Требуется дополнительное обращение к серверу активации.
89479413	Сервер активации вернул ошибку 643.
89479414	Сервер активации вернул ошибку 644.
89479415	Сервер активации вернул ошибку 645.
89479416	Сервер активации вернул ошибку 646.
89479417	Формат кода активации не поддерживается сервером активации.
89479418	Неверный формат кода активации.

89479419	На компьютере установлено некорректное системное время.
8947941A	Код активации не подходит для версии Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.
8947941B	Подписка истекла.
8947941C	Превышен предел количества активаций для данного лицензионного ключа.
8947941D	Неверная цифровая подпись лицензионного ключа.
8947941E	Требуются дополнительные данные пользователя.
8947941F	Проверка данных пользователя завершена с ошибкой.
89479420	Подписка неактивна.
89479421	Технические работы на сервере активации.
89479501	Неизвестная ошибка на стороне Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.
89479502	Передан недопустимый параметр (например, пустой список адресов серверов активации).
89479503	Неверный код активации.
89479504	Неверное имя пользователя.
89479505	Неверный пароль пользователя.
89479506	Сервер активации вернул неверный ответ.
89479507	Запрос на активацию прерван.
89479509	Сервер активации вернул пустой список переадресации.

Приложение. Профили программы

Профиль – компонент, задача или функция Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Профили предназначены для управления программой из командной строки. Вы можете использовать профили для выполнения команд `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` и `IMPORT`. С помощью профилей вы можете настроить параметры программы (например, `STOP DeviceControl`) или запустить задачу (например, `START Scan_My_Computer`).

Доступны следующие профили:

- `AdaptiveAnomaliesControl` – Адаптивный контроль аномалий.
- `AMSI` – Поставщик AMSI-защиты.
- `BehaviorDetection` – Анализ поведения.
- `DeviceControl` – Контроль устройств.
- `EntAppControl` – Контроль программ.
- `File_Monitoring` или `FM` – Защита от файловых угроз.
- `Firewall` или `FW` – Сетевой экран.
- `HIPS` – Предотвращение вторжений.
- `IDS` – Защита от сетевых угроз.
- `IntegrityCheck` – Проверка целостности.
- `Mail_Monitoring` или `EM` – Защита от почтовых угроз.
- `Rollback` – Откат обновления.
- `Scan_ContextScan` – Проверка из контекстного меню.
- `Scan_IdleScan` – Фоновая проверка.
- `Scan_Memory` – Проверка памяти ядра.
- `Scan_My_Computer` – Полная проверка.
- `Scan_Objects` – Выборочная проверка.
- `Scan_Qscan` – Проверка объектов, загрузка которых осуществляется при запуске операционной системы.
- `Scan_Removable_Drive` – Проверка съемных дисков.
- `Scan_Startup` или `STARTUP` – Проверка важных областей.
- `Updater` – Обновление.
- `Web_Monitoring` или `WM` – Защита от веб-угроз.
- `WebControl` – Веб-Контроль.

Также Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает работу служебных профилей. Служебные профили могут понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

Управление программой через REST API

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет настраивать параметры программы, запускать проверку и обновление антивирусных баз, а также выполнять другие задачи с помощью сторонних решений. Для этого Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предоставляет API. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready REST API работает по протоколу HTTP и представляет собой набор методов "запрос / ответ". То есть вы можете управлять Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через стороннее решение, а не локальный интерфейс программы или Консоль администрирования Kaspersky Security Center.

Для начала работы с REST API нужно установить Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с поддержкой REST API.RESTклиент и Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready должны быть установлены на одном компьютере. Управление программой через REST API осуществляется по адресу http://127.0.0.1 или http://localhost. Удаленно управлять Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через REST API невозможно.

ОТКРЫТЬ ДОКУМЕНТАЦИЮ REST API

Установка программы с REST API

Для управления программой через REST API нужно установить Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с поддержкой REST API. Если вы управляете Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через REST API, управлять программой с помощью Kaspersky Security Center невозможно.

Чтобы установить Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с поддержкой REST API, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready версии 11.2.0 или выше.
3. Установите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready со следующими параметрами:
   - `RESTAPI=1`
   - `RESTAPI_User=<Имя пользователя>`

     Имя пользователя для управления программой через REST API. Введите имя пользователя в формате `<DOMAIN>\<UserName>` (например, `RESTAPI_User=COMPANY\Administrator`). Вы можете управлять программой через REST API только под этой учетной записью. Для работы с REST API вы можете выбрать только одного пользователя.
   - `RESTAPI_Port=<Порт>`

     Порт для обмена данными. Необязательный параметр. По умолчанию выбран порт 6782.
   - `AdminKitConnector=1`

     Управление программой с помощью систем администрирования. По умолчанию управление разрешено.

Также вы можете задать параметры работы с REST API с помощью файла setup.ini.

Вы можете задать параметры работы с REST API только во время установки программы. Изменить параметры после установки программы невозможно. Если вы хотите изменить параметры, удалите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и установите заново с новыми параметрами работы с REST API.

Пример:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1
/pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator /s
```

В результате вы сможете управлять программой через REST API. Для проверки работы откройте документацию REST API с помощью GET-запроса.

Пример:

```
GET http://localhost:6782/kes/v1/api-docs
```

Работа с API

Ограничить доступ к программе через REST API с помощью Защиты паролем невозможно. Например, запретить выключать защиту через REST API невозможно. Вы можете настроить Защиту паролем через REST API и ограничить доступ пользователей к программе через локальный интерфейс.

Для управления программой через REST API нужно запустить REST-клиент под учетной записью, которую вы задали при установке программы с поддержкой REST API. Для работы с REST API вы можете выбрать только одного пользователя.

ОТКРЫТЬ ДОКУМЕНТАЦИЮ REST API

Управление программой через REST API состоит из следующих этапов:

1. Получите текущие значения параметров программы. Для этого отправьте GET-запрос.

   Пример:

   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. Программа отправит ответ со структурой и значениями параметров. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает XML- и JSON-форматы.

   Пример:

   ```
   {
   "action": 0, "enableSystemProcessesMemoryProtection": true, "enabled": true
   }
   ```

3. Измените параметры программы. Для этого отправьте POST-запрос. Используйте структуру параметров, полученную в ответ от GET-запроса.

Пример:

```
POST http://localhost:6782/kes/v1/settings/ExploitPrevention
{
"action": 0,
"enableSystemProcessesMemoryProtection": false,
"enabled": true
}
```

4. Программа применит изменения в параметрах и отправит ответ с результатами настройки программы.

Источники информации о программе

Страница Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Endpoint Security в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе.

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

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

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского".

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Получение информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на компьютере, подробные отчеты работы компонентов программы.

Во время работ по диагностике специалисты Службы технической поддержки могут попросить вас изменить параметры программы:

- Активировать функциональность получения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения полученной диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав полученных в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

О составе и хранении файлов трассировки

Вы сами несете ответственность за обеспечение безопасности полученной информации и, в частности, за контроль и ограничение доступа к полученной информации, хранимой на компьютере, до ее передачи в "Лабораторию Касперского".

Файлы трассировки хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы.

Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке %ProgramData%\Kaspersky Lab.

Файлы трассировки называются следующим образом: `KES<номер версии_dateXX.XX_timeXX.XX_pidXXX.><тип файла трассировки>.log`.

Вы можете просмотреть данные, записанные в файлы трассировки.

Все файлы трассировки содержат следующие общие данные:

- Время события.
- Номер потока выполнения.

  Эту информацию не содержит файл трассировки Агента аутентификации.

- Компонент программы, в результате работы которого произошло событие.
- Степень важности события (информационное, предупреждение, критическое, ошибка).
- Описание события выполнения команды компонента программы и результата выполнения этой команды.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет пароли пользователя в файл трассировки только в зашифрованном виде.

Содержание файлов трассировки SRV.log, GUI.log и ALL.log

В файлы трассировки `SRV.log`, `GUI.log` и `ALL.log`, помимо общих данных, может записываться следующая информация:

- Персональные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на локальном компьютере.
- Данные об установленном на компьютере аппаратном обеспечении (например, данные о прошивке BIOS / UEFI). Эти данные записываются в файлы трассировки при выполнении полнодискового шифрования по технологии Шифрование диска Kaspersky.
- Имя пользователя и пароль, если они передавались в открытом виде. Эти данные могут записываться в файлы трассировки при проверке интернет-трафика.
- Имя пользователя и пароль, если они содержатся в заголовках протокола HTTP.
- Имя учетной записи для входа в Microsoft Windows, если имя учетной записи является частью имени файла.
- Адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.
- Веб-сайты, которые вы посещаете, а также ссылки с этих веб-сайтов. Эти данные записываются в файлы трассировки, когда программа проверяет веб-сайты.
- Адрес прокси-сервера, имя компьютера, порт, IP-адрес, имя пользователя, используемое при авторизации на прокси-сервере. Эти данные записываются в файлы трассировки, если программа использует прокси-сервер.

- Внешние IP-адреса, с которыми было установлено соединение с вашего компьютера.
- Тема сообщения, идентификатор, имя отправителя и адрес веб-страницы отправителя сообщения в социальной сети. Эти данные записываются в файлы трассировки, если включен компонент ВебКонтроль.
- Данные о сетевом трафике. Эти данные записываются в файлы трассировки, если включены компоненты мониторинга трафика (например, Веб-Контроль).
- Данные, полученные с серверов "Лаборатории Касперского" (например, версия антивирусных баз).
- Статусы компонентов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и сведения об их работе.
- Данные о действиях пользователя в программе.
- События операционной системы.

Содержание файлов трассировки HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Файл трассировки `HST.log`, помимо общих данных, содержит информацию о выполнении задачи обновления баз и программных модулей.

Файл трассировки `BL.log`, помимо общих данных, содержит информацию о событиях, возникающих во время работы программы, а также данные, необходимые для устранения неполадок в работе программы. Этот файл создается, если программа запускается с параметром avp.exe –bl.

Файл трассировки `Dumpwriter.log`, помимо общих данных, содержит служебную информацию, необходимую для устранения неполадок, возникающих при записи файла дампа программы.

Файл трассировки `WD.log`, помимо общих данных, содержит информацию о событиях, возникающих в процессе работы службы avpsus, в том числе события обновления программных модулей.

Файл трассировки `AVPCon.dll.log`, помимо общих данных, содержит информацию о событиях, возникающих при работе модуля связи с Kaspersky Security Center.

Содержание файлов трассировки производительности

Файлы трассировки производительности называются следующим образом: `KES<номер версии_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Файлы трассировки производительности, помимо общих данных, содержат информацию о нагрузке на процессор, о времени загрузки операционной системы и программ, о запущенных процессах.

Содержание файла трассировки компонента Поставщик AMSI-защиты

Файл трассировки AMSI.log, помимо общих данных, содержит информацию о результатах проверок, запрошенных сторонними приложениями.

Содержание файла трассировки компонента Защита от почтовых угроз

Файл трассировки `mcou.OUTLOOK.EXE.log`, помимо общих данных, может содержать части сообщений электронной почты, в том числе адреса электронной почты.

Содержание файла трассировки компонента Проверка из контекстного меню

Файл трассировки `shellex.dll.log`, помимо общих данных, содержит информацию о выполнении задачи проверки и данные, необходимые для устранения неполадок в работе программы.

Содержание файлов трассировки веб-плагина программы

Файлы трассировки веб-плагина программы хранятся на компьютере, на котором развернута Kaspersky Security Center 12 Web Console, в папке Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 12\logs.

Файлы трассировки веб-плагина программы называются следующим образом: `logs-kes_windows-<тип файла трассировки>.DESKTOP-<дата обновления файла>.log`. Web Console начинает записывать данные после установки и удаляет файлы трассировки после удаления Web Console.

Файлы трассировки веб-плагина программы, помимо общих данных, содержат следующую информацию:

- Пароль пользователя KLAdmin для разблокировки интерфейса Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (Защита паролем).
- Временный пароль для разблокировки интерфейса Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready (Защита паролем).
- Имя пользователя и пароль для почтового SMTP-сервера (Уведомления по электронной почте).
- Имя пользователя и пароль для прокси-сервера сети интернет (Прокси-сервер).
- Имя пользователя и пароль для задачи Изменение состава компонентов программы.
- Учетные данные и пути, указанные в свойствах политики и в задачах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Содержание файла трассировки Агента аутентификации

Файл трассировки Агента аутентификации хранится в папке System Volume Information и называется следующим образом: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Файл трассировки Агента аутентификации, помимо общих данных, содержит информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации.

Трассировка работы программы

Трассировка программы – это подробная запись действий, выполняемых программой, и сообщений о событиях, происходящих во время работы программы.

Выполняйте трассировку программы под руководством Службы технической поддержки "Лаборатории Касперского".

Чтобы создать файл трассировки программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Поддержка.

   Откроется окно Поддержка.

2. В окне Поддержка нажмите на кнопку Трассировка системы.

   Откроется окно Информация для поддержки.

3. Чтобы запустить процесс трассировки, выберите один из следующих элементов в раскрывающемся списке Трассировка программы:

   - Включена.

     Выберите этот элемент, чтобы включить трассировку.

   - С ротацией.

     Выберите этот элемент, чтобы включить трассировку и ограничить максимальное количество файлов трассировки и максимальный размер каждого из файлов трассировки. Если записано максимальное количество файлов трассировки максимального размера, то удаляется наиболее старый файл трассировки и начинается запись нового файла трассировки.

     Если выбран этот элемент, вы можете указать значение для следующих полей:

     - Максимальное количество файлов для ротации.
     - Максимальный размер каждого файла.

4. В раскрывающемся списке Уровень выберите уровень трассировки.

   Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. Если указания Службы технической поддержки отсутствуют, рекомендуется устанавливать уровень трассировки Обычный (500).

5. Перезапустите Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

6. Чтобы остановить процесс трассировки, вернитесь в окно Информация для поддержки и выберите Выключена в раскрывающемся списке Трассировка программы.

Вы также можете создать файлы трассировки во время установки программы из командной строки, в том числе с помощью файла setup.ini.

Трассировка производительности программы

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет получить информацию о проблемах в работе компьютера при использовании программы. Например, вы можете получить информацию о задержках при загрузке операционной системы после установки программы. Для этого Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает файлы трассировки производительности. Трассировка производительности – это запись действий, выполняемых программой, для диагностики проблем производительности Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Для получения информации Kaspersky Endpoint Security для бизнеса -

Расширенный EDR Ready использует сервис трассировки событий Windows (англ. ETW – Event Tracing for Windows). Диагностику работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и установление причин возникновения проблем выполняет Служба технической поддержки "Лаборатории Касперского".

Выполняйте трассировку программы под руководством Службы технической поддержки "Лаборатории Касперского".

Чтобы создать файл трассировки производительности, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Поддержка.
2. В окне Поддержка нажмите на кнопку Трассировка системы.

   Откроется окно Информация для поддержки.
3. В раскрывающемся списке Трассировка производительности выберите элемент Включена или С ротацией.

   Ротация позволяет ограничить размер файла трассировки. Укажите максимальный размер файла трассировки. Если размер файла достигает максимального размера, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready перезаписывает наиболее старые строки в этом файле.
4. В раскрывающемся списке Уровень выберите уровень трассировки:
   - Легкий. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready анализирует основные процессы операционной системы, связанные с производительностью.
   - Детальный. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready анализирует все процессы операционной системы, связанные с производительностью.
5. В раскрывающемся списке Тип трассировки выберите тип трассировки:
   - Базовая информация. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready анализирует процессы во время работы операционной системы. Используйте этот тип трассировки, если проблема воспроизводится после загрузки операционной системы, например, проблема доступа в интернет в браузере.
   - При перезагрузке. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready анализирует процессы только на этапе загрузки операционной системы. После загрузки операционной системы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready останавливает трассировку. Используйте этот тип трассировки, если проблема связана с задержкой загрузки операционной системы.
6. Перезагрузите компьютер и воспроизведите проблему.
7. Чтобы остановить процесс трассировки, вернитесь в окно Информация для поддержки и выберите Выключена в раскрывающемся списке Трассировка производительности.

В результате в папке %ProgramData%\Kaspersky Lab будет создан файл трассировки производительности. После создания файла трассировки отправьте файл в Службу технической поддержки "Лаборатории Касперского".

Запись дампов

Сохраненные дампы могут содержать конфиденциальные данные. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту файлов дампов.

Файлы дампов хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. Файлы дампов хранятся в папке %ProgramData%\Kaspersky Lab.

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на момент создания этого файла дампа.

Чтобы включить или выключить запись дампов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры программы.
3. В блоке Отладочная информация нажмите на кнопку Настройка.

   Откроется окно Отладочная информация.
4. Выполните одно из следующих действий:
   - Установите флажок Включить запись дампов, если вы хотите чтобы программа записывала дампы программы.
   - Снимите флажок Включить запись дампов, если вы не хотите чтобы программа записывала дампы программы.
5. Нажмите на кнопку OK в окне Отладочная информация.
6. Нажмите на кнопку Сохранить в главном окне программы, чтобы сохранить внесенные изменения.

Защита файлов дампов и трассировок

Файлы дампов и файлы трассировки содержат информацию об операционной системе, а также могут содержать данные пользователя. Чтобы предотвратить несанкционированный доступ к этим данным, вы можете включить защиту файлов дампов и файлов трассировки.

Если защита файлов дампов и файлов трассировки включена, доступ к файлам имеют следующие пользователи:

- К файлам дампов имеют доступ системный и локальный администраторы, а также пользователь, включивший запись файлов дампов и файлов трассировки.
- К файлам трассировки имеют доступ только системный и локальный администраторы.

Чтобы включить или выключить защиту файлов дампов и файлов трассировки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку Настройка.
2. В окне параметров программы выберите раздел Общие параметры → Параметры программы.
3. В блоке Отладочная информация нажмите на кнопку Настройка.

   Откроется окно Отладочная информация.
4. Выполните одно из следующих действий:

   - Установите флажок Включить защиту файлов дампов и файлов трассировки, если вы хотите включить защиту.
   - Снимите флажок Включить защиту файлов дампов и файлов трассировки, если вы хотите выключить защиту.
5. Нажмите на кнопку OK в окне Отладочная информация.
6. Нажмите на кнопку Сохранить в главном окне программы, чтобы сохранить внесенные изменения.

Файлы дампов и файлы трассировки, записанные при включенной защите, остаются защищенными после отключения этой функции.

Глоссарий

OLE-объект

Файл, присоединенный или встроенный в другой файл. Программы "Лаборатории Касперского" позволяют проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft O ice Excel® в документ Microsoft O ice Word, данная таблица будет проверяться как OLE-объект.

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех программ "Лаборатории Касперского", работающих в операционной системе Windows. Для программ, работающих в других операционных системах, предназначены отдельные версии Агента администрирования.

Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами "Лаборатории Касперского", регулярно обновляется и входит в поставку программы "Лаборатории Касперского".

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые. База регулярно обновляется и входит в поставку программы "Лаборатории Касперского".

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Доверенный платформенный модуль

Микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины.

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Зараженный файл

Файл, внутри которого содержится вредоносный код (при проверке файла был обнаружен код известной программы, представляющей угрозу). Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими файлами, поскольку это может привести к заражению вашего компьютера.

Издатель сертификата

Центр сертификации, выдавший сертификат.

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

Ложное срабатывание

Ситуация, когда незараженный файл определяется программой "Лаборатории Касперского" как зараженный ввиду того, что его код напоминает код вируса.

Маска

Представление названия и расширения файла общими символами.

Для формирования маски файла можно использовать любые символы, допустимые в названиях файлов, в том числе специальные:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске C, но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папке `Folder` и вложенных папках. Маска `C:\**\*.txt` не работает. Маска ** доступна только для создания исключений из проверки.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Нормализованная форма адреса веб-ресурса

Нормализованной формой адреса веб-ресурса называется текстовое представление адреса веб-ресурса, полученное в результате применения нормализации. Нормализация – процесс, в результате которого текстовое представление адреса веб-ресурса изменяется в соответствии с определенными правилами (например, исключение из текстового представления адреса веб-ресурса имени пользователя, пароля и порта соединения, понижение верхнего регистра символов адреса веб-ресурса до нижнего регистра).

В контексте работы компонентов защиты цель нормализации адресов веб-ресурсов заключается в том, чтобы проверять синтаксически различные, но физически эквивалентные адреса веб-ресурсов один раз.

Пример:

Ненормализованная форма адреса: www.Example.com\.

Нормализованная форма адреса: www.example.com.

Область защиты

Объекты, которые компонент базовой защиты постоянно проверяет во время своей работы. Область защиты разных компонентов имеет разные свойства.

Область проверки

Объекты, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет во время выполнения задачи проверки.

Портативный файловый менеджер

Программа, предоставляющая интерфейс для работы с зашифрованными файлами на съемных дисках при недоступности функциональности шифрования на компьютере.

Резервный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Приложение 1. Параметры политики в Web Console и Cloud Console

Вы можете настроить параметры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с помощью политики. Подробная информация о компонентах программы приведена в соответствующих подразделах.

Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready получает от служб KSN сведения о категории и репутации проверяемых файлов, а также сведения о репутации проверяемых вебадресов.

Использование Kaspersky Security Network является добровольным. Программа предлагает использовать KSN во время первоначальной настройки программы. Начать или прекратить использование KSN можно в любой момент.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского". Файл ksn_<ID языка>.txt с текстом Положения о Kaspersky Security Network входит в комплект поставки программы.

Для снижения нагрузки на серверы KSN специалисты "Лаборатории Касперского" могут выпускать обновления для программы, которые временно выключают или частично ограничивают обращения в Kaspersky Security Network. В этом случае статус подключения к KSN в локальном интерфейсе программы – Включено с ограничениями.

Инфраструктура KSN

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает следующие инфраструктурные решения KSN:

- Глобальный KSN – это решение, которое используют большинство программ "Лаборатории Касперского".

Участники KSN получают информацию от Kaspersky Security Network, а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз Kaspersky Security Network.

- Локальный KSN – это решение, позволяющее пользователям компьютеров, на которые установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready или другие программы "Лаборатории Касперского", получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров. Локальный KSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky
  - Security Network, например, по следующим причинам: отсутствие подключения локальных рабочих мест к сети Интернет;
  -

  законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

По умолчанию Kaspersky Security Center использует Глобальный KSN. Вы можете настроить использование Локального KSN в Консоли администрирования (MMC) и Kaspersky Security Center 12 Web Console. Настроить использование Локального KSN в Kaspersky Security Center Cloud Console невозможно.

Подробнее о работе Локального KSN см. в документации для Kaspersky Private Security Network.

KSN Proxy

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.

- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал связи с внешней сетью и ускоряя получение компьютером пользователя запрошенной информации.

Подробную информацию о службе KSN Proxy см. в справке Kaspersky Security Center.

Параметры Kaspersky Security Network

Параметр	Описание
Расширенный режим KSN	Расширенный режим KSN – режим работы программы, при котором Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready передает в "Лабораторию Касперского" дополнительные данные. Независимо от положения переключателя, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует KSN для обнаружения угроз.

Облачный режим	Облачный режим – режим работы программы, при котором Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует облегченную версию антивирусных баз. Работу программы с облегченными антивирусными базами обеспечивает Kaspersky Security Network. Облегченная версия антивирусных баз позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready загружает полную версию антивирусных баз с серверов "Лаборатории Касперского". Если переключатель включен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует облегченную версию антивирусных баз, за счет чего снижается нагрузка на ресурсы операционной системы. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready загружает облегченную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был установлен. Если переключатель выключен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует полную версию антивирусных баз. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready загружает полную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был снят.
Статус компьютера при недоступности серверов KSN	Раскрывающийся список, элементы которого определяют статус компьютера в Kaspersky Security Center при недоступности серверов KSN (Устройства → Управляемые устройства).
Использовать KSN Proxy	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует службу KSN Proxy. Вы можете настроить параметры службы KSN Proxy в свойствах Сервера администрирования.
Использовать серверы KSN при недоступности KSN Proxy	Если флажок установлен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует серверы KSN, когда служба KSN Proxy недоступна. Серверы KSN могут быть расположены как на стороне "Лаборатории Касперского", в случае использования Глобального KSN, так и на сторонних серверах, в случае использования Локального KSN.

Анализ поведения

Компонент Анализ поведения получает данные о действиях программ на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы.

Компонент Анализ поведения использует шаблоны опасного поведения программ. Если активность программы совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

Параметры компонента Анализ поведения

Параметр	Описание
При обнаружении вредоносной активности программы	• Удалять файл. Если выбран этот вариант, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready удаляет исполняемый файл вредоносной программы и создает резервную копию файла в резервном хранилище. • Завершать работу программы. Если выбран этот вариант, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready завершает работу этой программы. • Информировать. Если выбран этот вариант, то в случае обнаружения вредоносной активности программы, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не завершает работу этой программы и добавляет информацию о вредоносной активности этой программы в список активных угроз.
Защита папок общего доступа от внешнего шифрования	Если переключатель включен, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready анализирует активность в папках общего доступа. Если активность совпадает с одним из шаблонов опасного поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready выполняет выбранное действие. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready защищает от попыток внешнего шифрования только те файлы, которые расположены на носителях информации с файловой системой NTFS и не зашифрованы системой EFS.
При обнаружении внешнего шифрования папок общего доступа	• Информировать. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз. • Блокировать соединение. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready блокирует сетевую активность компьютера, осуществляющего изменение, и создает резервные копии измененных файлов. Если включен компонент Откат вредоносных действий и выбран вариант Блокировать соединение, то выполняется восстановление измененных файлов из резервных копий.
Блокировать соединение на N минут	Время, на которое Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready блокирует сетевую активность удаленного компьютера, осуществляющего шифрование папок общего доступа.

Исключения	Список компьютеров, с которых не будут отслеживаться попытки шифрования папок общего доступа. Для работы списка исключений компьютеров из защиты папок общего доступа от внешнего шифрования требуется включить аудит входа в систему в политике аудита безопасности Windows. По умолчанию аудит входа в систему выключен. Подробнее о политике аудита безопасности Windows см. на сайте Microsoft).

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимую программу. При обработке этих данных уязвимая программа выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО.

Если попытка запустить исполняемый файл из уязвимой программы не была произведена пользователем, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует запуск этого файла или информирует пользователя.

Параметры компонента Защита от эксплойтов

Параметр	Описание
При обнаружении эксплойта	• Блокировать операцию. Если выбран этот вариант, то, обнаружив эксплойт, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует действия этого эксплойта. • Информировать. Если выбран этот вариант, то в случае обнаружения эксплойта Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не блокирует действия эксплойта и добавляет информацию об этом эксплойте в список активных угроз.
Защита памяти системных процессов	Если переключатель включен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует сторонние процессы, осуществляющие попытки доступа к памяти системных процессов.

Предотвращение вторжений

Компонент Предотвращение вторжений (англ. HIPS – Host Intrusion Prevention System) предотвращает выполнение программами опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным. Компонент обеспечивает защиту компьютера с помощью антивирусных баз и облачной службы Kaspersky Security Network.

Компонент контролирует работу программ с помощью прав программ. Права программ включают в себя следующие параметры доступа:

- доступ к ресурсам операционной системы (например, параметры автозапуска, ключи реестра);
- доступ к персональным данным (например, к файлам, программам).

Сетевую активность программ контролирует Сетевой экран с помощью сетевых правил.

Во время первого запуска программы компонент Предотвращение вторжений выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.
2. Проверяет безопасность программы в Kaspersky Security Network.

   Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает программу в одну из групп доверия: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

   Группа доверия определяет права, которые Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready использует для контроля сетевой активности программ. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

   Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает программу в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

   Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует действия программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещен доступ к модулям операционной системы.

При следующем запуске программы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие права программ. Если программа была изменена, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready исследует программу как при первом запуске.

Параметры компонента Предотвращение вторжений

Параметр	Описание

Права программ	Программы Таблица программ, работу которых контролирует компонент Предотвращение вторжений. Программы распределены по группам доверия. Группа доверия определяет права, которые Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready использует для контроля активности программ. Вы можете выбрать программу из единого списка всех программ, установленных на компьютерах под действием политики, и добавить программу в группу доверия. Права доступа программы приведены в следующих таблицах: • Файлы и системный реестр. Таблица, которая содержит права доступа программ, входящих в группу доверия, к ресурсам операционной системы и персональным данным. • Права. Таблица, которая содержит права доступа программ, входящих в группу доверия, к процессам и ресурсам операционной системы. • Сетевые правила. Таблица сетевых правил программ, входящих в группу доверия. В соответствии с этими правилами Сетевой экран регулирует сетевую активность для программ. В таблице отображаются предустановленные сетевые правила, которые рекомендованы специалистами "Лаборатории Касперского". Эти сетевые правила добавлены для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Windows. Удалить предустановленные сетевые правила невозможно.
Защищаемые ресурсы	Имя Таблица содержит ресурсы компьютера, распределенные по категориям. Компонент Предотвращение вторжений контролирует доступ других программ к ресурсам из этой таблицы. Ресурсом может быть категория реестра, файл или папка, ключ реестра. Программы Таблица программ, работу которых контролирует компонент Предотвращение вторжений, для выбранного ресурса. Программы распределены по группам доверия. Группа доверия определяет права, которые Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready использует для контроля активности программ.
Программы, запускаемые до Kaspersky Endpoint Security для Windows, автоматически помещаются в группу доверия	Группа доверия, в которую Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready будет помещать программы, запускаемые до Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready.
Обновлять права для ранее неизвестных программ из базы KSN	Если флажок установлен, то компонент Предотвращение вторжений обновляет права ранее неизвестных программ, используя базы Kaspersky Security Network.

Доверять программам, имеющим цифровую подпись	Если флажок установлен, то компонент Предотвращение вторжений помещает программы, имеющие цифровую подпись, в группу "Доверенные". Если флажок снят, компонент Предотвращение вторжений не считает программы с цифровой подписью доверенными и распределяет их по группам доверия на основании других параметров.
Удалять права для программ, не запускавшихся более чем N дней	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически удаляет информацию о программе (группа доверия, права доступа) при выполнении следующих условий: • Вы вручную поместили программу в группу доверия или настроили права доступа. • Программа не запускалась в течении заданного периода времени. Если группа доверия и права программы определены автоматически, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет информацию об этой программе через 30 дней. Изменить время хранения информации о программе или выключить автоматическое удаление невозможно. При следующем запуске этой программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready исследует программу как при первом запуске.
Программы, для которых не удалось определить группу доверия, автоматически помещать в <группа доверия>	Раскрывающийся список, элементы которого определяют, в какую группу доверия Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет помещать неизвестную программу. Вы можете выбрать один из следующих элементов: • Слабые ограничения. • Сильные ограничения. • Недоверенные.

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполнить откат действий, произведенных вредоносными программами в операционной системе.

Во время отката действий вредоносной программы в операционной системе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обрабатывает следующие типы активности вредоносной программы:

- Файловая активность

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

  - удаляет исполняемые файлы, созданные вредоносной программой (на всех носителях, кроме сетевых дисков);
  - удаляет исполняемые файлы, созданные программами, в которые внедрилась вредоносная программа;
  - восстанавливает измененные или удаленные вредоносной программой файлы.

Функциональность восстановления файлов имеет ряд ограничений.

- Реестровая активность

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

  - удаляет разделы и ключи реестра, созданные вредоносной программой; не восстанавливает
  - измененные или удаленные вредоносной программой разделы и ключи реестра.

- Системная активность

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

  - завершает процессы, которые запускала вредоносная программа;
  - завершает процессы, в которые внедрялась вредоносная программа;
  - не возобновляет процессы, которые остановила вредоносная
  - программа.

  Сетевая активность

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие

  - действия: запрещает сетевую активность вредоносной программы; запрещает сетевую
  - активность тех процессов, в которые внедрялась вредоносная программа.

Откат действий вредоносной программы может быть запущен компонентом Защита от файловых угроз, Анализ поведения или при антивирусной проверке.

Откат действий вредоносной программы затрагивает строго ограниченный набор данных. Откат не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз постоянно находится в оперативной памяти компьютера. Компонент проверяет файлы на всех дисках компьютера, а также на подключенных дисках. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент проверяет файлы, к которым обращается пользователь или программа. При обнаружении вредоносного файла Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует операцию с файлом. Далее программа лечит или удаляет вредоносный файл, в зависимости от настройки компонента Защита от файловых угроз.

При обращении к файлу, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready загружает и проверяет содержимое этого файла.

Параметры компонента Защита от файловых угроз

Параметр	Описание
Область защиты	Содержит объекты, которые проверяет компонент Защита от файловых угроз. Объектом проверки может быть жесткий, съемный или сетевой диск, папка, файл или несколько файлов, определенных по маске. По умолчанию компонент Защита от файловых угроз проверяет файлы, запускаемые со всех жестких, съемных и сетевых дисков. Область защиты этих объектов невозможно изменить или удалить. Вы можете только исключить объект (например, съемные диски) из проверки.
Действие при обнаружении угрозы	Лечить; удалять, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready их удаляет. Лечить; блокировать, если лечение невозможно. Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз блокирует эти файлы. Блокировать. Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически блокирует зараженные файлы без попытки их вылечить. Перед лечением или удалением зараженного файла компонент Защита от файловых угроз формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.
Проверять только новые и измененные файлы	Флажок включает / выключает режим проверки только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки.
Проверять архивы	Флажок включает / выключает проверку архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних программ.
Проверять файлы офисных форматов	Флажок включает / выключает проверку файлов Microsoft O ice (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
Не распаковывать составные файлы большого размера	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет составные файлы любого размера. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок Не распаковывать составные файлы большого размера.
Распаковывать	

составные файлы в фоновом режиме	Если флажок установлен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предоставляет доступ к составным файлам, размер которых превышает заданное значение, до проверки этих файлов. При этом Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в фоновом режиме распаковывает и проверяет составные файлы. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предоставляет доступ к составным файлам, размер которых меньше данного значения, только после распаковки и проверки этих файлов. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предоставляет доступ к составным файлам только после распаковки и проверки файлов любого размера.

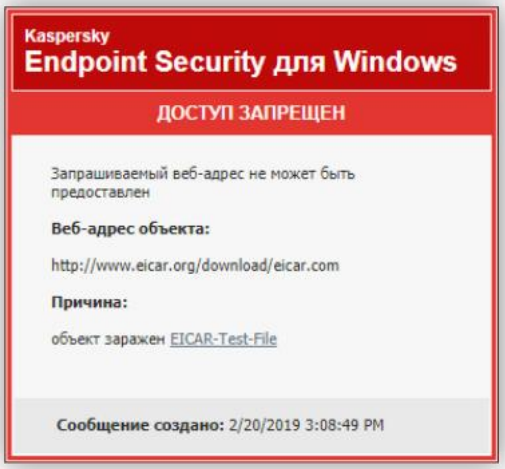
Защита от веб-угроз

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует вредоносные и фишинговые веб-сайты. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет HTTP-, HTTPS- и FTP-трафик. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет URL- и IP-адреса. Вы можете задать порты, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет контролировать, или выбрать все порты.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

При попытке пользователя открыть вредоносный или фишинговый веб-сайт, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует доступ и покажет предупреждение (см. рис. ниже).



Сообщение о запрете доступа к веб-сайту

Параметры компонента Защита от веб-угроз

Параметр	Описание

Действие при обнаружении угрозы	• Запрещать загрузку. Если выбран этот вариант, то в случае обнаружения в вебтрафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере. • Информировать. Если выбран этот вариант, то в случае обнаружения в вебтрафике зараженного объекта, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает загрузку этого объекта на компьютер и добавляет информацию о зараженном объекте в список активных угроз.
Не проверять веб-трафик с доверенных веб-адресов	Если флажок установлен, компонент Защита от веб-угроз не проверяет содержимое веб-страниц / веб-сайтов, адреса которых включены в список доверенных веб-адресов.
Доверенные веб-адреса	Компонент Защита от веб-угроз не проверяет содержимое веб-страниц / веб-сайтов, адреса которых включены в список доверенных веб-адресов. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта.

Защита от почтовых угроз

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других программ, представляющих угрозу. Также компонент проверяет сообщения на наличие вредоносных и фишинговых ссылок. По умолчанию компонент Защита от почтовых угроз постоянно находится в оперативной памяти компьютера и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, NNTP или в почтовом клиенте Microsoft O ice Outlook (MAPI). Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready переименовывает тему сообщения: `[Сообщение заражено] <тема сообщения>` или `[Зараженный объект удален] <тема сообщения>`.

Компонент взаимодействует с почтовыми клиентами, установленными на компьютере. Для почтового клиента Microsoft O ice Outlook предусмотрено расширение с дополнительными параметрами. Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft O ice Outlook во время установки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Параметры компонента Защита от почтовых угроз

Параметр	Описание

Действие при обнаружении угрозы	Лечить; удалять, если лечение невозможно. При обнаружении зараженного объекта во входящем или исходящем сообщении Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет зараженный объект. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавит информацию о выполненном действии в тему сообщения: `[Зараженный объект удален] <тема сообщения>`. Лечить; блокировать, если лечение невозможно. При обнаружении зараженного объекта во входящем сообщении Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Если вылечить объект не удалось, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует отправку сообщения, почтовый клиент показывает ошибку. Запрещать. При обнаружении зараженного объекта во входящем сообщении Kaspersky Endpoint Security добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует отправку сообщения, почтовый клиент показывает ошибку.
Трафик POP3 / SMTP / NNTP / IMAP	Флажок включает / выключает проверку компонентом Защита от почтовых угроз почтового трафика, проходящего по протоколам POP3, SMTP, NNTP и IMAP.
Расширение в Microsoft O ice Outlook	Если флажок установлен, включена проверка сообщений электронной почты, передающихся по протоколам POP3, SMTP, NNTP, IMAP на стороне расширения, интегрированного в Microsoft O ice Outlook. В случае проверки почты с помощью расширения для Microsoft O ice Outlook рекомендуется использовать режим кеширования Exchange (Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендации по его использованию вы можете найти в базе знаний Microsoft.
Не проверять архивы размером более N МБ	Если флажок установлен, компонент Защита от почтовых угроз исключает из проверки вложенные в сообщения электронной почты архивы, размер которых больше заданного. Если флажок снят, компонент Защита от почтовых угроз проверяет архивы любого размера, вложенные в сообщения электронной почты.
Не проверять архивы более N сек	Если флажок установлен, то время проверки архивов, вложенных в сообщения электронной почты, ограничено указанным периодом.

Фильтр вложений	Фильтр вложений не работает для исходящих сообщений электронной почты. Не применять фильтр. Если выбран этот вариант, компонент Защита от почтовых угроз не фильтрует файлы, вложенные в сообщения электронной почты. Переименовывать вложения указанных типов. Если выбран этот вариант, компонент Защита от почтовых угроз в именах вложенных файлов указанных типов заменяет последний символ на символ подчеркивания (например, attachment_.docx). Удалять вложения указанных типов. Если выбран этот вариант, компонент Защита от почтовых угроз удаляет из сообщений электронной почты вложенные файлы указанных типов. Типы вложенных файлов, которые нужно переименовывать или удалять из сообщений электронной почты, вы можете указать в списке масок файлов.

Защита от сетевых угроз

Компонент Защита от сетевых угроз (англ. IDS – Intrusion Detection System) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует сетевое соединение с атакующим компьютером.

Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей программы.

Параметры компонента Защита от сетевых угроз

Параметр	Описание
Добавить атакующий компьютер в список блокирования на N минут	Если флажок установлен, то компонент Защита от сетевых угроз добавляет атакующий компьютер в список блокирования. Это означает, что компонент Защита от сетевых угроз блокирует сетевое соединение с атакующим компьютером после первой попытки сетевой атаки в течение заданного времени, чтобы автоматически защитить компьютер пользователя от возможных будущих сетевых атак с этого адреса.
Исключения	Список содержит IP-адреса, сетевые атаки с которых компонент Защита от сетевых угроз не блокирует. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не заносит в отчет информацию о сетевых атаках с IPадресов, входящих в список исключений.
Защита от MAC-спуфинга	Атака типа MAC-спуфинг заключается в изменении MAC-адреса сетевого устройства (сетевой карты). В результате злоумышленник может перенаправить данные, отправленные на устройство, на другое устройство и получить доступ к этим данным. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет блокировать атаки MAC-спуфинга и получать уведомления об атаках.

Сетевой экран

Сетевой экран блокирует несанкционированные подключения к компьютеру во время работы в интернете или локальной сети. Также Сетевой экран контролирует сетевую активность программ на компьютере. Это позволяет защитить локальную сеть организации от кражи персональных данных и других атак. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и предустановленных сетевых правил.

Сетевые правила

Вы можете настроить сетевые правила на следующих уровнях:

- Сетевые пакетные правила. Используются для ввода ограничений на сетевые пакеты независимо от программы. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready имеет предустановленные сетевые пакетные правила с разрешениями, рекомендованными специалистами "Лаборатории Касперского".

- Сетевые правила программ. Используются для ограничения сетевой активности конкретной программы. Учитываются не только характеристики сетевого пакета, но и конкретная программа, которой адресован этот сетевой пакет, либо которая инициировала отправку этого сетевого пакета.

Контроль доступа программ к ресурсам операционной системы, процессам и персональным данным обеспечивает компонент Предотвращение вторжений с помощью прав программ.

Во время первого запуска программы Сетевой экран выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.

2. Проверяет безопасность программы в Kaspersky Security Network.

   Для более эффективной работы Сетевого экрана вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает программу в одну из групп доверия: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

   Группа доверия определяет права, которые Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready использует для контроля сетевой активности программ. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает программу в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready помещает программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует сетевую активность программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещены любые сетевые соединения.

При следующем запуске программы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие сетевые правила. Если программа была изменена, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready исследует программу как при первом запуске.

Приоритеты сетевых правил

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если сетевая активность добавлена в несколько правил, Сетевой экран регулирует сетевую активность по правилу с высшим приоритетом.

Сетевые пакетные правила имеют более высокий приоритет, чем сетевые правила программ. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила программ, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Сетевые пакетные правила имеют более высокий приоритет, чем сетевые правила программ. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила программ, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Сетевые правила программ имеют особенность. Сетевые правило программ включает в себя правила доступа по статусу сети: публичная, локальная, доверенная. Например, для группы доверия "Сильные ограничения" по умолчанию запрещена любая сетевая активность программы в сетях всех статусов. Если для отдельной программы (родительская программа) задано сетевое правило, то дочерние процессы других программ будут выполнены в соответствии с сетевым правилом родительской программы. Если сетевое правило для программы отсутствует, дочерние процессы будут выполнены в соответствии с правилом доступа к сетям группы доверия.

Например, вы запретили любую сетевую активность всех программ для сетей всех статусов, кроме браузера X. Если в браузере X (родительская программа) запустить установку браузера Y (дочерний процесс), то установщик браузера Y получит доступ к сети и загрузит необходимые файлы. После установки браузеру Y будут запрещены любые сетевые соединения в соответствии с параметрами Сетевого экрана. Чтобы запретить установщику браузера Y сетевую активность в качестве дочернего процесса, необходимо добавить сетевое правило для установщика браузера Y.

Статусы сетевых соединений

Сетевой экран позволяет контролировать сетевую активность в зависимости от статуса сетевого соединения. Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready получает статус сетевого соединения от операционной системы компьютера. Статус сетевого соединения в операционной системе задает пользователь при настройке подключения. Вы можете изменить статус сетевого соединения в параметрах Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Сетевой экран будет контролировать сетевую активность в зависимости от статуса сети в параметрах Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready, а не операционной системы.

Выделены следующие статусы сетевого соединения:

- Публичная сеть. Сеть не защищена антивирусными программами, сетевыми экранами, фильтрами (например, Wi-Fi в кафе). Пользователю компьютера, подключенного к такой сети, Сетевой экран закрывает доступ к файлам и принтерам этого компьютера. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу

этого компьютера. Сетевой экран фильтрует сетевую активность каждой программы в соответствии с сетевыми правилами этой программы.

Сетевой экран по умолчанию присваивает статус Публичная сеть сети Интернет. Вы не можете изменить статус сети Интернет.

- Локальная сеть. Сеть для пользователей, которым ограничен доступ к файлам и принтерам этого компьютера (например, для локальной сети организации или для домашней сети).

Доверенная сеть. Безопасная сеть, во время работы в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. Для сетей с этим статусом Сетевой экран разрешает любую сетевую активность в рамках этой сети.

Параметры компонента Сетевой экран

Параметр	Описание
Сетевые пакетные правила	Таблица сетевых пакетных правил. Сетевые пакетные правила используются для ввода ограничений на сетевые пакеты независимо от программы. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. В таблице представлены предустановленные сетевые пакетные правила, которые рекомендованы специалистами "Лаборатории Касперского" для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Microsoft Windows. Сетевой экран устанавливает приоритет выполнения для каждого сетевого пакетного правила. Сетевой экран обрабатывает сетевые пакетные правила в порядке их расположения в списке сетевых пакетных правил, сверху вниз. Сетевой экран находит первое по порядку подходящее для сетевого соединения сетевое пакетное правило и выполняет его действие: либо разрешает, либо блокирует сетевую активность. Далее Сетевой экран игнорирует все последующие сетевые пакетные правила для данного сетевого соединения. Сетевые пакетные правила имеют приоритет над сетевыми правилами программ.
Сетевые соединения	Таблица, содержащая информацию о сетевых соединениях, которые Сетевой экран обнаружил на компьютере пользователя. Сети Интернет по умолчанию присвоен статус Публичная сеть. Вы не можете изменить статус сети Интернет.

Сетевые правила	Приложения Таблица программ, работу которых контролирует компонент Сетевой экран. Программы распределены по группам доверия. Группа доверия определяет права, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует для контроля сетевой активности программ. Вы можете выбрать программу из единого списка всех программ, установленных на компьютерах под действием политики, и добавить программу в группу доверия. Сетевые правила Таблица сетевых правил программ, входящих в группу доверия. В соответствии с этими правилами Сетевой экран регулирует сетевую активность для программ. В таблице отображаются предустановленные сетевые правила, которые рекомендованы специалистами "Лаборатории Касперского". Эти сетевые правила добавлены для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Windows. Удалить предустановленные сетевые правила невозможно.

Защита от атак BadUSB

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру.

Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USBустройств, имитирующих клавиатуру.

Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, программа предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный программой. Эта процедура называется авторизацией клавиатуры. Программа разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

Компонент Защита от атак BadUSB не устанавливается по умолчанию. Если вам нужен компонент Защита от атак BadUSB, вы можете добавить компонент в свойствах инсталляционного пакета перед установкой программы или измените состав компонентов программы после установки программы.

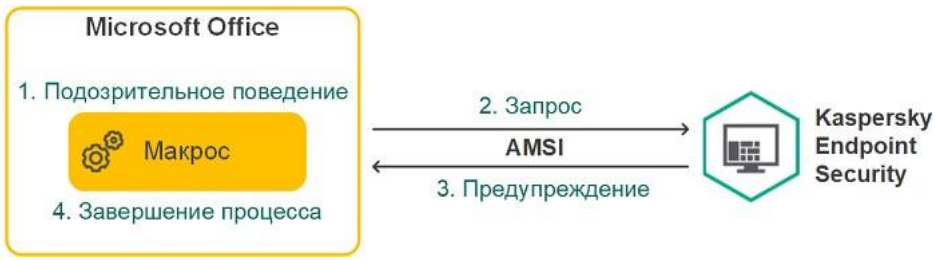
Параметры компонента Защита от атак BadUSB

Параметр	Описание
Запрет на использование экранной клавиатуры для авторизации USB-устройств	Если флажок установлен, программа запрещает использование экранной клавиатуры для авторизации USB-устройства, с которого невозможно ввести код авторизации.

Поставщик AMSI-защиты

Поставщик AMSI-защиты предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft. Интерфейс Antimalware Scan Interface (AMSI) позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для дополнительной проверки и получать результаты проверки этих объектов. Сторонними приложениями могут быть, например, программы Microsoft O ice (см. рис. ниже). Подробнее об интерфейсе AMSI см. в документации Microsoft.

Поставщик AMSI-защиты может только обнаруживать угрозу и уведомлять стороннее приложение об обнаруженной угрозе. Стороннее приложение после получения уведомления об угрозе не дает выполнить вредоносные действия (например, завершает работу).



Пример работы AMSI

Компонент Поставщик AMSI-защиты может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправляет информацию об отклонении запроса от стороннего приложения на Сервер администрирования. Компонент Поставщик AMSI-защиты не отклоняет запросы от тех сторонних приложений, для которых установлен флажок Не блокировать взаимодействие с Поставщиком AMSIзащиты.

Поставщик AMSI-защиты доступен для следующих операционных систем рабочих станций и серверов:

- Windows 10 Home / Pro / Education / Enterprise;
- Windows Server 2016 Essentials / Standard /
- Datacenter;

Windows Server 2019 Essentials / Standard / Datacenter.

Параметры компонента Поставщик AMSI-защиты

Параметр	Описание
Проверять архивы	Флажок включает / выключает проверку архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних программ.
Проверять файлы офисных форматов	Флажок включает / выключает проверку файлов Microsoft O ice (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
Не распаковывать составные файлы большого размера	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет составные файлы любого размера. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок Не распаковывать составные файлы большого размера.

Контроль программ

Контроль программ управляет запуском программ на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании программ. Также Контроль программ снижает риск заражения компьютера, ограничивая доступ к программам.

Настройка Контроля программ состоит из следующих этапов:

1. Создание категорий программ.

   Администратор создает категории программ, которыми администратор хочет управлять. Категории программ предназначены для всех компьютеров сети организации независимо от групп администрирования. Для создания категории вы можете использовать следующие критерии: KL-категория (например, Браузеры), хеш файла, производитель программы и другие.

2. Создание правил Контроля программ.

   Администратор создает правила Контроля программ в политике для группы администрирования. Правило включает в себя категории программ и статус запуска программ из этих категорий: запрещен или разрешен.

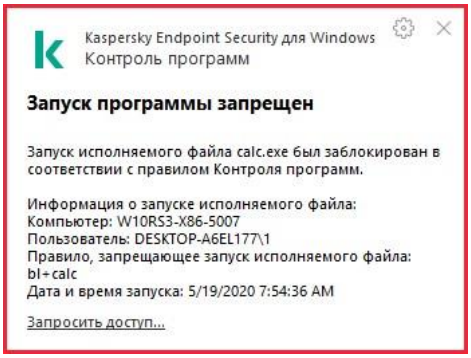
3. Выбор режима работы Контроля программ.

   Администратор выбирает режим работы с программами, которые не входят ни в одно из правил: черный и белый списки.

При попытке пользователя запустить запрещенную программу, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует запуск программы и покажет уведомление (см. рис. ниже).

Для проверки настройки Контроля программ предусмотрен тестовый режим. В этом режиме Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

- разрешает запуск программ, в том числе запрещенных;
- показывает уведомление о запуске запрещенной программы и добавляет информацию в отчет на компьютере пользователя; • отправляет данные о запуске запрещенных программ в Kaspersky Security Center.



Уведомление Контроля программ

Режимы работы Контроля программ

Компонент Контроль программ может работать в двух режимах:

- Черный список. Режим, при котором Контроль программ разрешает пользователям запуск любых программ, кроме тех, которые запрещены в правилах Контроля программ.

  Этот режим работы Контроля программ установлен по умолчанию.

- Белый список. Режим, при котором Контроль программ запрещает пользователям запуск любых программ, кроме тех, которые разрешены и не запрещены в правилах Контроля программ.

  Если разрешающие правила Контроля программ сформированы максимально полно, компонент запрещает запуск всех новых программ, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

  Вы можете ознакомиться с рекомендациями по настройке правил контроля программ в режиме белого списка.

Настройка Контроля программ для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, так и с помощью Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и необходимые для следующих задач:

- Создание категорий программ.

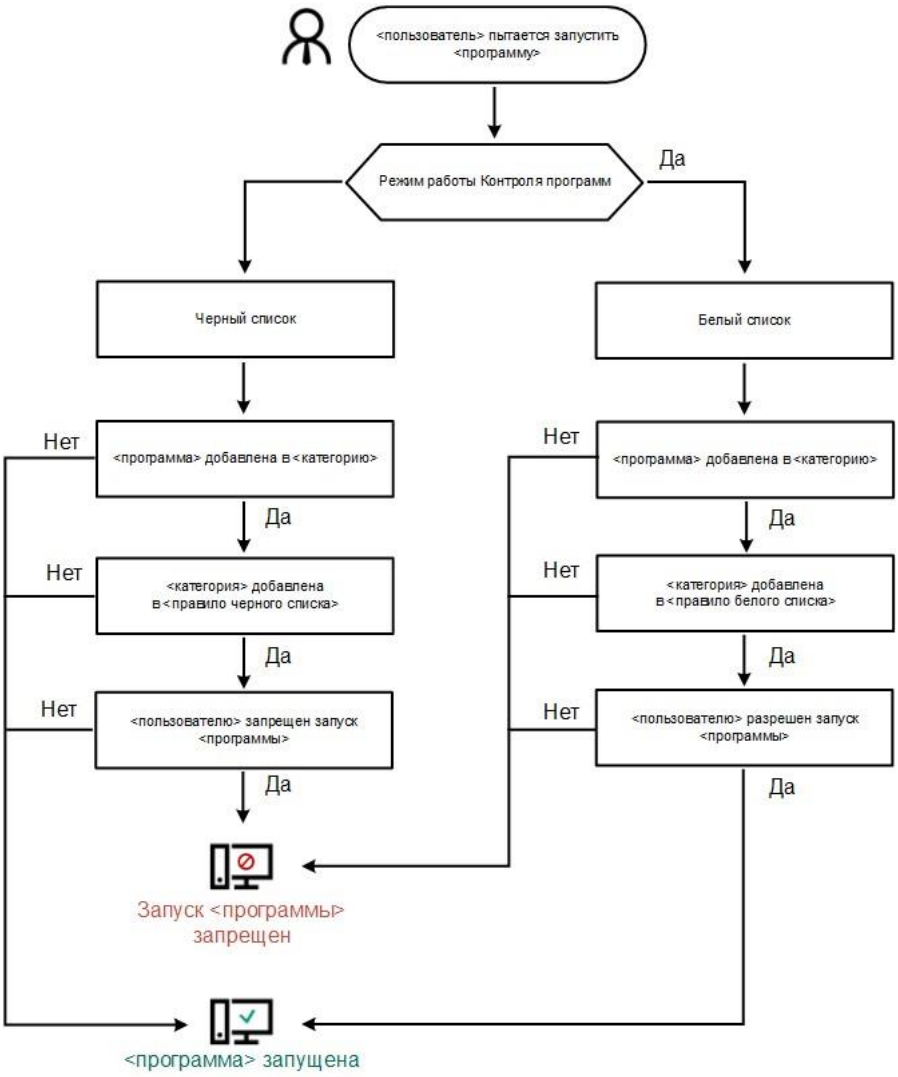
  Правила Контроля программ, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях программ, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

- Получение информации о программах, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль программ рекомендуется выполнять с помощью Kaspersky Security Center.

Алгоритм работы Контроля программ

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует алгоритм для принятия решения о запуске программы (см. рис. ниже).



Алгоритм работы Контроля программ

Параметры компонента Контроль программ

Параметр	Описание
Тестовый режим	Если переключатель включен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает запуск программы, запрещенной в текущем режиме Контроля программ, но заносит информацию о ее запуске в отчет.

Режим Контроля программ	Вы можете выбрать один из следующих вариантов: • Черный список. Если выбран этот вариант, Контроль программ разрешает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля программ. • Белый список. Если выбран этот вариант, Контроль программ запрещает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям разрешающих правил Контроля программ. При выборе режима Белый список автоматически создается два правила Контроля программ: • Операционная система и ее компоненты. • Доверенные программы обновления. Изменение параметров и удаление автоматически созданных правил недоступно. Вы можете включить или выключить эти правила.
Контролировать DLL и драйверы	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует загрузку DLLмодулей при запуске пользователями программ. Информация о DLL-модуле и программе, загрузившей этот DLL-модуль, сохраняется в отчет. При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля программ включено правило по умолчанию Операционная система и ее компоненты или другое правило, которое содержит KL-категорию "Доверенные сертификаты" и обеспечивает загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле Операционная система и ее компоненты может привести к нестабильности операционной системы. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует только DLL-модули и драйверы, загруженные с момента установки флажка Контролировать DLL и драйверы. Рекомендуется перезагрузить компьютер после установки флажка Контролировать DLL и драйверы, чтобы программа контролировала все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.
Шаблоны сообщений	Блокировка. Шаблон сообщения, которое появляется при срабатывании правила Контроля программ, блокирующего запуск программы. Сообщение администратору. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка программы, по мнению пользователя, произошла ошибочно.

Контроль устройств

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Контроль устройств управляет доступом пользователей к установленным или подключенным к компьютеру устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных.

Уровни доступа к устройствам

Контроль устройств управляет доступом на следующих уровнях:

- Тип устройства. Например, принтеры, съемные диски, CD/DVD-приводы.

  Вы можете настроить доступ устройств следующим образом:

  - Разрешать – ✓.
  - Запрещать – ⊘.
  - Зависит от шины подключения (кроме Wi-Fi) – .
  - Запрещать с исключениями (только Wi-Fi и портативные устройства (MTP)) – .

- Шина подключения. Шина подключения – интерфейс, с помощью которого устройства подключаются к компьютеру (например, USB, FireWire). Таким образом, вы можете ограничить подключение всех устройств, например, через USB.

  Вы можете настроить доступ устройств следующим образом:

  - Разрешать – ✓.
  - Запрещать – ⊘.

- Доверенные устройства. Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

  Вы можете добавить доверенные устройства по следующим данным:

  - Устройства по идентификатору. Каждое устройство имеет уникальный идентификатор (англ. Hardware ID – HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы. Пример идентификатора устройства: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств.
  - Устройства по модели. Каждое устройство имеет идентификатор производителя (англ. Vendor ID – VID) и идентификатор продукта(англ. Product ID – PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы. Шаблон для ввода VID и PID: `VID_1234&PID_5678`. Добавлять устройства по модели удобно, если вы используете в вашей

организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.

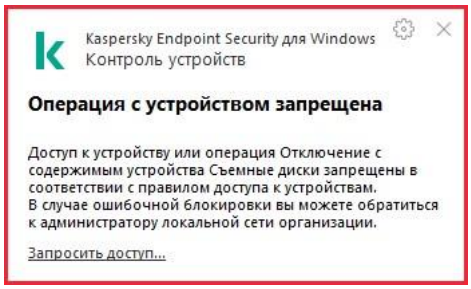
- Устройства по маске идентификатора. Если вы используете несколько устройств с похожими идентификаторами, вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не поддерживает символ ? при вводе маски. Например, `WDC_C*`.

- Устройства по маске модели. Если вы используете несколько устройств с похожими VID или PID (например, устройства одного производителя), вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не поддерживает символ `?` при вводе маски. Например, `VID_05AC&PID_*`.

Контроль устройств регулирует доступ пользователей к устройствам с помощью правил доступа. Также Контроль устройств позволяет сохранять события подключения / отключения устройств. Для сохранения событий вам нужно настроить отправку событий в политике.

Если доступ к устройству зависит от шины подключения (статус), Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не сохраняет события подключения / отключения устройства. Чтобы программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняла события подключения / отключения устройства, разрешите доступ к соответствующему типу устройств (статус ✓) или добавьте устройство в список доверенных.

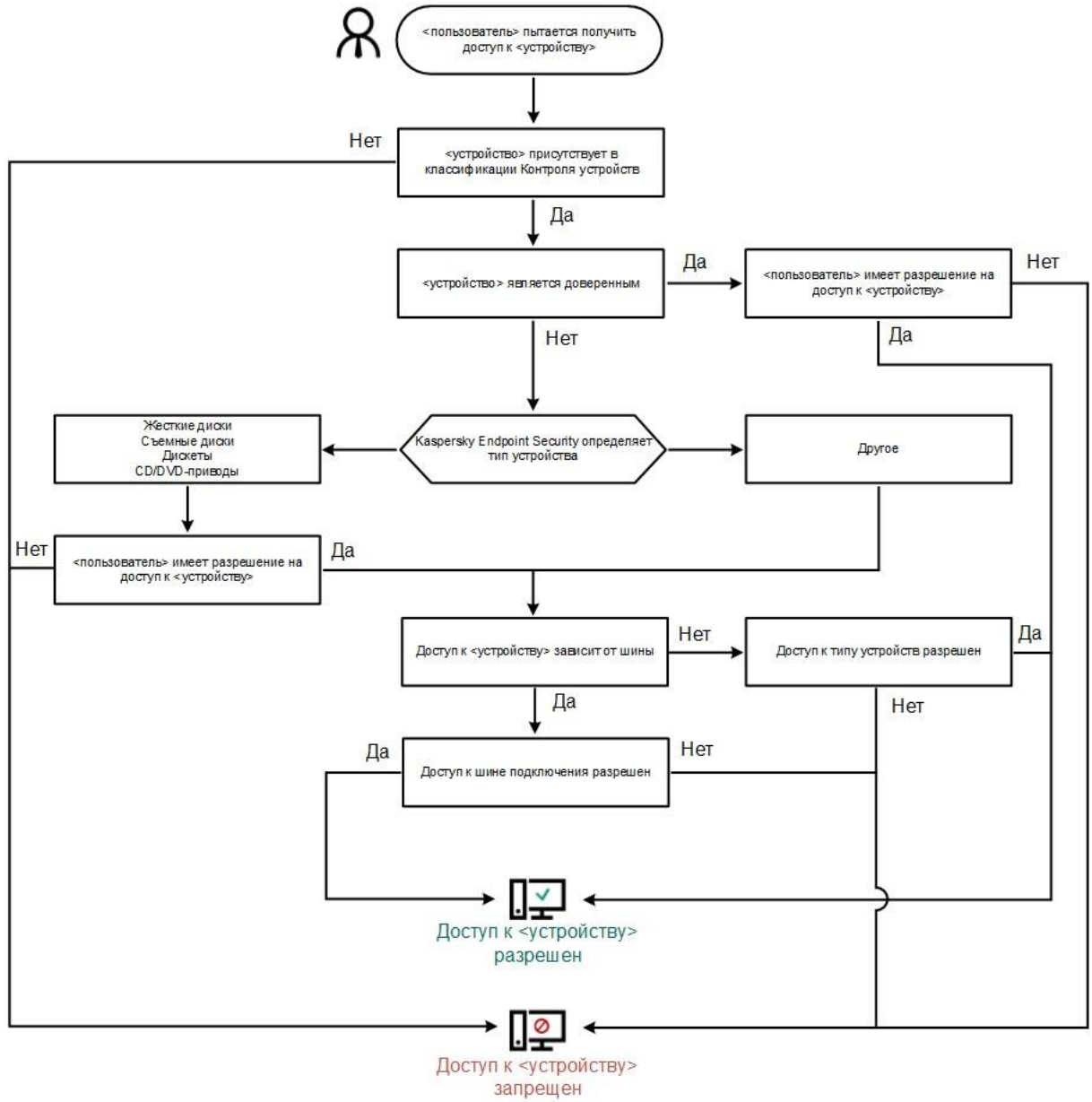
При подключении к компьютеру устройства, доступ к которому запрещен Контролем устройств, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует доступ и покажет уведомление (см. рис. ниже).



Уведомление Контроля устройств

Алгоритм работы Контроля устройств

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready принимает решение о доступе к устройству после того, как пользователь подключил это устройство к компьютеру (см. рис. ниже).



Алгоритм работы Контроля устройств

Если устройство подключено и доступ разрешен, вы можете изменить правило доступа и запретить доступ. В этом случае при очередном обращении к устройству (просмотр дерева папок, чтение, запись) Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready блокирует доступ. Блокирование устройства без файловой системы произойдет только при последующем подключении устройства.

Если пользователю компьютера с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready требуется запросить доступ к устройству, которое, по его мнению, было заблокировано ошибочно, передайте ему инструкцию по запросу доступа.

Параметры компонента Контроль устройств

Параметр	Описание
Разрешить запрашивать временный доступ	Если флажок установлен, то кнопка Запросить доступ в локальном интерфейсе Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready доступна. При нажатии на эту кнопку открывается окно Запрос доступа к устройству. С помощью этого окна пользователь может запросить временный доступ к заблокированному устройству.

Правила доступа для устройств и сетей Wi-Fi	Таблица со всеми возможными типами устройств по классификации компонента Контроль устройств и статусом доступа к ним.
Запретить подключение мобильных устройств в режимах ADB и iTunes	Параметры контроля доступа к мобильным устройствам под управлением Android и iOS относятся к параметрам портативных устройств (MTP). При подключении мобильного устройства к компьютеру операционная система определяет тип устройства. Если на компьютере установлены программы Android Debug Bridge (ADB), iTunes или их аналоги, операционная система определяет мобильные устройства как ADB- или iTunesустройства. В остальных случаях операционная система может определить тип мобильного устройства как портативное устройство (MTP) для передачи файлов, PTPустройство (камера) для передачи изображений или другое устройство. Тип устройства зависит от модели мобильного устройства. Если флажок установлен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запрещает доступ к мобильному устройству с помощью ADB и iTunes. При этом пользователь может заряжать батарею мобильного устройства. Доступ к мобильному устройству как к портативному устройству (MTP) или PTP-устройству (камера) регулируется правилом доступа для этого типа устройств. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready регулирует доступ к мобильным устройствам с помощью ADB и iTunes правилами доступа для портативных устройств (MTP) и PTP-устройств (камера). При этом, даже если доступ к портативным устройствам (MTP) запрещен, пользователь может заряжать батарею мобильного устройства.
Шины подключения	Список всех возможных шин подключения по классификации компонента Контроль устройств и статусом доступа к ним.
Доверенные устройства	Список доверенных устройств и пользователей, которым разрешен доступ к этим устройствам.
Анти-Бриджинг	Анти-Бриджинг предотвращает создание сетевых мостов, исключая возможность одновременной установки нескольких сетевых соединений для компьютера. Это позволяет защитить корпоративную сеть от атак через незащищенные, несанкционированные сети. Анти-Бриджинг блокирует установку нескольких соединений в соответствии с приоритетами устройств. Чем выше находится устройство в списке, тем выше его приоритет. Если активное и новое соединения относятся к одному типу (например, Wi-Fi), Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует активное соединение и разрешает установку нового соединения. Если активное и новое соединения относятся к разным типам (например, сетевой адаптер и Wi-Fi), Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует соединение с более низким приоритетом и разрешает соединение с более высоким приоритетом. Анти-Бриджинг поддерживает работу со следующими типами устройств: сетевой адаптер, Wi-Fi и модем.

Шаблоны сообщений	• Блокировка. Шаблон сообщения, которое появляется при обращении пользователя к заблокированному устройству. Также сообщение появляется при попытке пользователя совершить операцию над содержимым устройства, которая запрещена для этого пользователя. • Сообщение администратору. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к устройству или запрет операции над содержимым устройства, по мнению пользователя, произошли ошибочно.

Веб-Контроль

Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть вебсайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует доступ или покажет предупреждение (см. рис. ниже).

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready контролирует только HTTP- и HTTPS-трафик.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

Способы управления доступом к веб-сайтам

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- Категория веб-сайта. Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз программы). Вы можете ограничить доступ пользователей, например, к категории "Социальные сети" или другим категориям.
- Тип данных. Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready определяет тип данных по формату файла, а не по расширению.

  Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready определит тип данных "Архивы", а не "Графические файлы".

- Отдельный адрес. Вы можете ввести веб-адрес или использовать маски.

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к типу данных "Файлы офисных программ" только для категории веб-сайтов "Веб-почта".

Правила доступа к веб-сайтам

Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью правил доступа. Вы можете настроить следующие дополнительные параметры правила доступа к веб-сайтам:

- Пользователи, на которых распространяется правило.

  Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

- Расписание работы правила.

  Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Приоритеты правил доступа

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом. Например, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории веб-сайтов "Социальные сети" и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.

Сообщения Веб-Контроля

Параметры компонента Веб-Контроль

Параметр	Описание

Список правил	Список с правилами доступа к веб-ресурсам. Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом.
Правило по умолчанию	Правило по умолчанию – правило доступа к веб-ресурсам, которые не входят ни в одно из правил. Возможны следующие варианты: • Разрешать все, не указанное в списке правил – режим черного списка. • Запрещать все, не указанное в списке правил – режим белого списка.
Шаблоны сообщений	• Предупреждение. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу. • Блокировка. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу. • Сообщение администратору. Поле ввода содержит шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно.
Записывать данные о посещении разрешенных страниц в журнал	Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready записывает данные о посещении всех веб-сайтов, в том числе и разрешенных. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправляет события в Kaspersky Security Center, локальный журнал Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, журнал событий Windows. Для мониторинга активности пользователя в интернете нужно настроить параметры сохранения событий. Мониторинг активности пользователя в интернете может потребовать больше ресурсов компьютера при расшифровке HTTPS-трафика.

Адаптивный контроль аномалий

Вы можете управлять Адаптивным контролем аномалий в Kaspersky Security Center 12 Web Console. Управлять Адаптивным контролем аномалий в программе Kaspersky Security Center Cloud Console невозможно. Также вы можете управлять Адаптивным контролем аномалий в Консоли администрирования Kaspersky Security Center.

Компонент Адаптивный контроль аномалий доступен только для продуктов Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для бизнеса Расширенный и Kaspersky Total Security для бизнеса (более подробная информация о продуктах Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для бизнеса доступна на сайте "Лаборатории Касперского").

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Адаптивный контроль аномалий отслеживает и блокирует действия, нехарактерные для компьютеров сети организации. Для отслеживания нехарактерных действий Адаптивный контроль аномалий использует набор правил (например, правило Запуск Windows PowerShell из офисной программы). Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил и, например, разрешить запуск PowerShell-скриптов для автоматизации решения корпоративных задач. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обновляет набор правил с базами программы. Обновление набора правил нужно подтверждать вручную.

Настройка Адаптивного контроля аномалий

Настройка Адаптивного контроля аномалий состоит из следующих этапов:

1. Обучение Адаптивного контроля аномалий.

   После включения Адаптивного контроля аномалий правила работают в обучающем режиме. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил и отправляет события срабатывания в Kaspersky Security Center. Каждое правило имеет свой срок действия обучающего режима. Срок действия обучающего режима устанавливают специалисты "Лаборатории Касперского". Обычно срок действия обучающего режима составляет 2 недели.

   Если в ходе обучения правило ни разу не сработало, Адаптивный контроль аномалий будет считать действия, связанные с этим правилом, нехарактерным. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready будет блокировать все действия, связанные с этим правилом.

   Если в ходе обучения правило сработало, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready регистрирует события в отчете о срабатываниях правил и в хранилище Срабатывание правил в обучающем режиме.

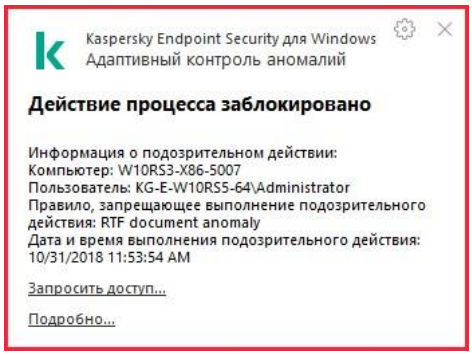
2. Анализ отчета о срабатывании правил.

   Администратор анализирует отчет о срабатываниях правил или содержание хранилища Срабатывание правил в обучающем режиме. Далее администратор может выбрать поведение Адаптивного контроля аномалий при срабатывании правила: блокировать или разрешить. Также администратор может продолжить отслеживать срабатывание правила и продлить работу программы в обучающем режиме. Если администратор не предпринимает никаких мер, программа также продолжит работать в обучающем режиме. Отсчет срока действия обучающего режима начинается заново.

Настройка Адаптивного контроля аномалий происходит в режиме реального времени. Настройка Адаптивного контроля аномалий осуществляется по следующим каналам:

- Адаптивный контроль аномалий автоматически начинает блокировать действия, связанные с правилами, которые не сработали в течение обучающего режима.
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавляет новые правила или удаляет неактуальные.
- Администратор настраивает работу Адаптивного контроля аномалий после анализа отчета о срабатывании правил и содержимого хранилища Срабатывание правил в обучающем режиме. Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища Срабатывание правил в обучающем режиме.

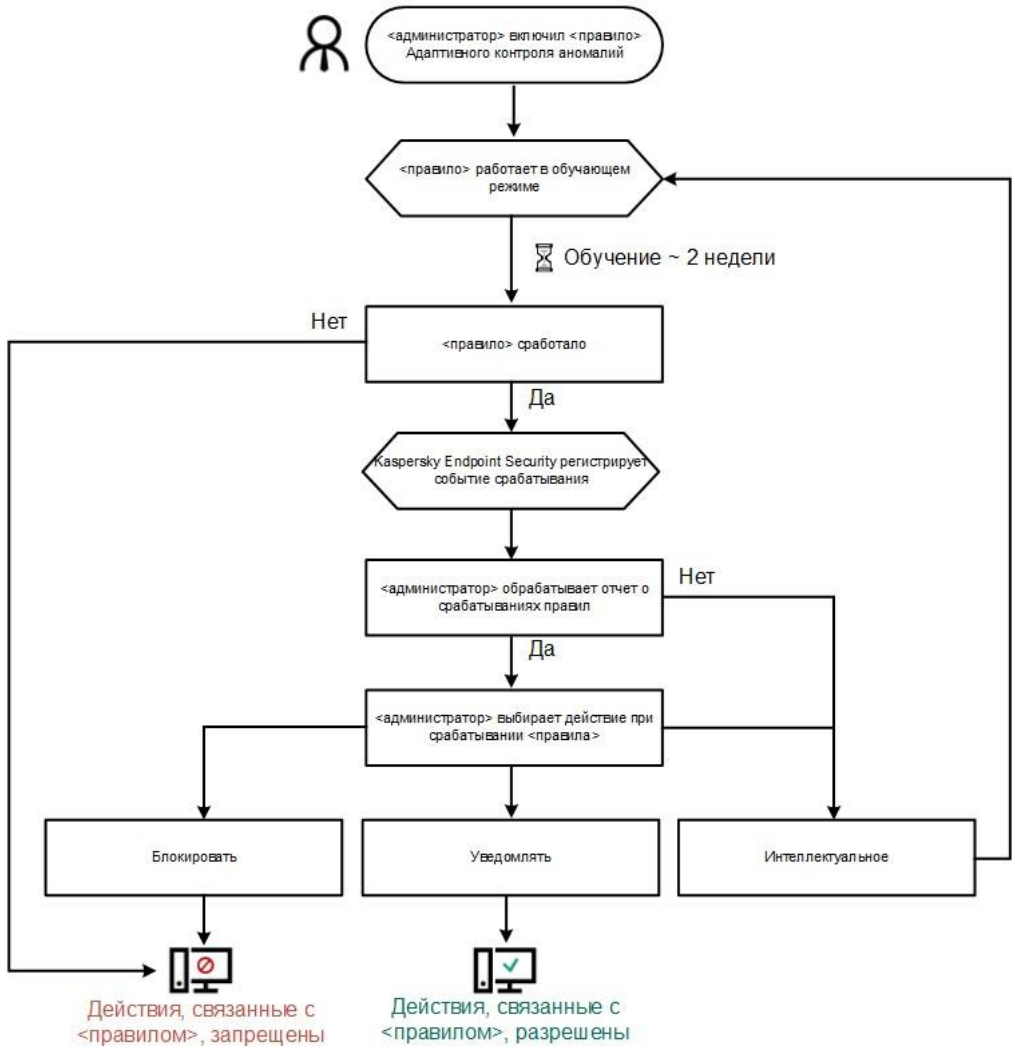
При попытке вредоносной программы выполнить действие, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready заблокирует действие и покажет уведомление (см. рис. ниже).



Уведомление Адаптивного контроля аномалий

Алгоритм работы Адаптивного контроля аномалий

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready принимает решение о выполнении действия, связанного с правилом, по следующему алгоритму (см. рис. ниже).



Алгоритм работы Адаптивного контроля аномалий

Параметры компонента Адаптивный контроль аномалий

Параметр	Описание

Отчет о состоянии правил	В этом отчете содержится информация о статусе правил обнаружения Адаптивного контроля аномалий (например, статусы Выключено или Блокировать). Отчет формируется для всех групп администрирования.
Отчет о срабатываниях правил	В этом отчете содержится информация о нехарактерных действиях, обнаруженных с помощью Адаптивного контроля аномалий. Отчет формируется для всех групп администрирования.
Правила	Таблица правил Адаптивного контроля аномалий. Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев потенциально вредоносной активности.
Шаблоны сообщений	• Блокировка. Шаблон сообщения для пользователя, которое появляется при срабатывании правила Адаптивного контроля аномалий, блокирующего нехарактерное действие. • Сообщение администратору. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка действия, по мнению пользователя, произошла ошибочно.

Полнодисковое шифрование

Вы можете выбрать технологию шифрования: Шифрование диска Kaspersky или Шифрование диска BitLocker (далее также "BitLocker").

Шифрование диска Kaspersky

После шифрования системных жестких дисков при последующем включении компьютера доступ к ним, а также загрузка операционной системы возможны только после прохождения процедуры аутентификации с помощью Агента аутентификации. Для этого требуется ввести пароль токена или смарт-карты, подключенных к компьютеру, или имя и пароль учетной записи Агента аутентификации, созданной системным администратором локальной сети организации с помощью задачи Управления учетными записями Агента
аутентификации. Эти учетные записи основаны на учетных записях пользователей Microsoft Windows, под которыми пользователи выполняют вход в операционную систему. Также вы можете использовать технологию единого входа (англ. Single Sign-On – SSO), позволяющую осуществлять автоматический вход в операционную систему с помощью имени и пароля учетной записи Агента аутентификации.

Аутентификация пользователя в Агенте аутентификации может выполняться двумя способами:

• путем ввода имени и пароля учетной записи Агента аутентификации, созданной
администратором локальной сети организации средствами Kaspersky Security Center; • путем
ввода пароля подключенного к компьютеру токена или смарт-карты.

> Использование токена или смарт-карты доступно, только если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES256. Если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES56, то в добавлении файла электронного сертификата в команду будет отказано.

Шифрование диска BitLocker

BitLocker – встроенная в операционную систему Windows технология шифрования. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет контролировать и управлять Bitlocker с помощью Kaspersky Security Center. BitLocker шифрует логический том. Шифрование съемных дисков с помощью BitLocker невозможно. Подробнее о BitLocker см. в документации Microsoft.

BitLocker обеспечивает безопасность хранения ключей доступа с помощью доверенного платформенного модуля. Доверенный платформенный модуль (англ. Trusted Platform Module – TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины. Использование TPM является самым безопасным способом хранения ключей доступа BitLocker, так как TPM позволяет проверять целостность операционной системы. На компьютерах без TPM вы также можете зашифровать диски. При этом ключ доступа будет зашифрован паролем. Таким образом, BitLocker использует следующие способы аутентификации:

- TPM и пароль.
- TPM и PIN-код.
- Пароль.

После шифрования диска BitLocker создает мастер-ключ. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправляет мастерключ в Kaspersky Security Center, чтобы вы имели возможность восстановить доступ к диску, если пользователь, например, забыл пароль. Если пользователь самостоятельно зашифровал диск с помощью BitLocker, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отправит информацию о шифровании диска в Kaspersky Security Center. При этом Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не отправит мастер-ключ в Kaspersky Security Center, и восстановить доступ к диску с помощью Kaspersky Security Center будет невозможно. Для корректной работы BitLocker с Kaspersky Security Center расшифруйте диск и зашифруйте диск повторно с помощью политики. Расшифровать диск вы можете локально или с помощью политики.

После шифрования системного жесткого диска для загрузки операционной системы пользователю нужно пройти процедуру аутентификации BitLocker. После прохождения процедуры аутентификации BitLocker будет доступен вход в систему. BitLocker не поддерживает технологию единого входа (SSO).

Если вы используете групповые политики для Windows, выключите управление BitLocker в параметрах политики. Параметры политики для Windows могут противоречить параметрам политики Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. При шифровании диска могут возникнуть ошибки.

Параметры компонента Шифрование диска Kaspersky

Параметр	Описание

Режим шифрования	Шифровать все жесткие диски. Если выбран этот элемент, то при применении политики программа шифрует все жесткие диски. Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой установлена программа. Расшифровывать все жесткие диски. Если выбран этот элемент, то при применении политики программа расшифровывает все зашифрованные ранее жесткие диски. Оставлять без изменений. Если выбран этот элемент, то при применении политики программа оставляет диски в прежнем состоянии. Если диск был зашифрован, то он остается зашифрованным, а если диск был расшифрован, то он остается расшифрованным. Этот элемент выбран по умолчанию.

Автоматически создавать учетные записи Агента аутентификации для пользователей	Флажок включает / выключает автоматическое создание учетных записей Агента аутентификации при применении политики. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready формирует список учетных записей Агента аутентификации на основе учетных записей Windows. По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует все локальные и доменные учетные записи, с помощью которых пользователь выполнял вход в операционную систему за последние 30 дней.
Параметры создания учетных записей Агента аутентификации	Все учетные записи компьютера. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает учетные записи Агента аутентификации для всех учетных записей компьютера, которые когдалибо были активными. Все доменные учетные записи компьютера. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает учетные записи Агента аутентификации для всех учетных записей компьютера, которые принадлежат какому-либо домену и которые когда-либо были активными. Все локальные учетные записи компьютера. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает учетные записи Агента аутентификации для всех локальных учетных записей компьютера, которые когда-либо были активными. Локальный администратор. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает учетную запись локального администратора. Менеджер компьютера. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает учетную запись Агента аутентификации для учетной записи, в свойствах которой в Active Directory указано, что она является управляющей. Активная учетная запись. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически создает учетную запись Агента аутентификации для активной в момент выполнения задачи учетной записи компьютера.

Сохранять введенное в Агенте аутентификации имя пользователя	Если флажок установлен, то программа сохраняет имя учетной записи Агента аутентификации. При последующей аутентификации в Агенте аутентификации под той же учетной записью имя учетной записи вводить не требуется.
Шифровать только занятое пространство	Флажок включает / выключает функцию, ограничивающую область шифрования только занятыми секторами жесткого диска. Это ограничение позволяет сократить время шифрования. Включение / выключение функции Шифровать только занятое пространство после запуска шифрования не изменяет этого параметра до тех пор, пока жесткие диски не будут расшифрованы. Требуется установить или снять флажок до начала шифрования. Если флажок установлен, то шифруется только та часть жесткого диска, которая занята файлами. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь жесткий диск, в том числе остатки удаленных и отредактированных ранее файлов. Данную функцию рекомендуется применять для новых жестких дисков, данные которых не редактировались и не удалялись. Если вы применяете шифрование на уже используемом жестком диске, рекомендуется зашифровать весь жесткий диск. Это гарантирует защиту всех данных – даже удаленных, но потенциально восстанавливаемых. По умолчанию флажок снят.
Использовать Legacy USB Support	Флажок включает / выключает функцию Legacy USB Support. Legacy USB Support – функция BIOS / UEFI, которая позволяет использовать USB-устройства (например, токен) на этапе загрузки компьютера до запуска операционной системы (BIOSрежим). Функция Legacy USB Support не влияет на поддержку USB-устройств после запуска операционной системы. Если флажок установлен, то будет включена поддержка USB-устройств на этапе начальной загрузки компьютера. При включенной функции Legacy USB Support Агент аутентификации в BIOSрежиме не поддерживает работу с токенами по USB. Функцию рекомендуется использовать только при возникновении проблемы несовместимости с аппаратным обеспечением и только для тех компьютеров, на которых возникла проблема.

Параметры паролей	Параметры надежности пароля учетной записи Агента аутентификации. Также вы можете включить использование технологии единого входа (SSO). Технология единого входа позволяет использовать одни и те же учетные данные для доступа к зашифрованным жестким дискам и для входа в операционную систему. Если флажок установлен, то для доступа к зашифрованным жестким дискам и последующего автоматического входа в операционную систему требуется ввести учетные данные доступа к зашифрованным дискам. Если флажок снят, то для доступа к зашифрованным жестким дискам и последующего входа в операционную систему требуется отдельно ввести учетные данные для доступа к зашифрованным жестким дискам и учетные данные пользователя в операционной системе.
Справочные тексты	Аутентификация. Справочный текст, который отображается в окне Агента аутентификации на этапе ввода учетных данных. Смена пароля. Справочный текст, который отображается в окне Агента аутентификации на этапе смены пароля для учетной записи Агента аутентификации. Восстановление пароля. Справочный текст, который отображается в окне Агента аутентификации на этапе восстановления пароля для учетной записи Агента аутентификации.

Параметры компонента Шифрование диска BitLocker

Параметр	Описание
Режим шифрования	Шифровать все жесткие диски. Если выбран этот элемент, то при применении политики программа шифрует все жесткие диски. Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой установлена программа.
	Расшифровывать все жесткие диски. Если выбран этот элемент, то при применении политики программа расшифровывает все зашифрованные ранее жесткие диски. Оставлять без изменений. Если выбран этот элемент, то при применении политики программа оставляет диски в прежнем состоянии. Если диск был зашифрован, то он остается зашифрованным, а если диск был расшифрован, то он остается расшифрованным. Этот элемент выбран по умолчанию.

Включить использование проверки подлинности BitLocker, требующей предзагрузочного ввода с клавиатуры на планшетах	Флажок включает / выключает использование аутентификации, требующей ввода данных в предзагрузочной среде, даже если у платформы отсутствует возможность предзагрузочного ввода (например, у сенсорных клавиатур на планшетах). Сенсорная клавиатура планшетов недоступна в предзагрузочной среде. Для прохождения аутентификации BitLocker на планшетах пользователю необходимо подключить, например, USB-клавиатуру. Если флажок установлен, то использование аутентификации, требующей предзагрузочного ввода, разрешено. Рекомендуется использовать этот параметр только для устройств, у которых во время предварительной загрузки, помимо сенсорных клавиатур, имеются альтернативные средства ввода данных, например, USB-клавиатура. Если флажок снят, шифрование диска BitLocker на планшетах невозможно.
Использовать аппаратное шифрование	Если флажок установлен, то программа применяет аппаратное шифрование. Это позволяет увеличить скорость шифрования и сократить использование ресурсов компьютера.
Шифровать только занятое пространство	Флажок включает / выключает функцию, ограничивающую область шифрования только занятыми секторами жесткого диска. Это ограничение позволяет сократить время шифрования. Включение / выключение функции Шифровать только занятое пространство после запуска шифрования не изменяет этого параметра до тех пор, пока жесткие диски не будут расшифрованы. Требуется установить или снять флажок до начала шифрования. Если флажок установлен, то шифруется только та часть жесткого диска, которая занята файлами. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь жесткий диск, в том числе остатки удаленных и отредактированных ранее файлов. Данную функцию рекомендуется применять для новых жестких дисков, данные которых не редактировались и не удалялись. Если вы применяете шифрование на уже используемом жестком диске, рекомендуется зашифровать весь жесткий диск. Это гарантирует защиту всех данных – даже удаленных, но потенциально восстанавливаемых. По умолчанию флажок снят.
Параметры аутентификации	Использовать доверенный платформенный модуль (TPM)

Если выбран этот вариант, BitLocker использует доверенный платформенный модуль (TPM).

Доверенный платформенный модуль (англ. Trusted Platform Module – TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины.

> Для компьютеров под управлением операционных систем Windows 7 и Windows Server 2008 R2 доступно только шифрование с использованием модуля TPM. Если модуль TPM не установлен, шифрование BitLocker невозможно. Использование пароля на этих компьютерах не поддерживается.

Устройство, оснащенное доверенным платформенным модулем, может создавать ключи шифрования, которые могут быть расшифрованы только с его помощью. Доверенный платформенный модуль шифрует ключи шифрования собственным корневым ключом хранилища. Корневой ключ хранилища хранится внутри доверенного платформенного модуля. Это обеспечивает дополнительную степень защиты ключей шифрования от попыток взлома.

Этот вариант действия выбран по умолчанию.

Вы можете настроить параметры доступа к ключу шифрования:

- Использовать PIN-код. Если флажок установлен, пользователь может использовать PIN-код для получения доступа к ключу шифрования, который хранится в доверенном платформенном модуле (TPM).
  Если флажок снят, пользователю запрещено использовать PIN-код. Для получения доступа к ключу шифрования пользователь использует пароль.

- Использовать пароль, если доверенный платформенный модуль (TPM) недоступен. Если флажок установлен, то при отсутствии доверенного платформенного модуля (TPM) пользователь может получить доступ к ключам шифрования с помощью пароля.
  Если флажок снят и модуль TPM недоступен, то полнодисковое шифрование не запускается.
  Использовать пароль

  Если выбран этот вариант, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запрашивает у пользователя пароль при обращении к зашифрованному диску.

  Этот вариант действия может быть выбран, если не используется доверенный платформенный модуль (TPM).

Шифрование файлов

Вы можете сформировать списки из файлов по расширению или группам расширений и из папок, расположенных на локальных дисках компьютера, а также создать правила шифрования файлов, создаваемых отдельными программами. После применения политики программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует и расшифровывает следующие файлы:

- файлы, отдельно добавленные в списки для шифрования и расшифровки;

- файлы, хранящиеся в папках, добавленных в списки для шифрования и расшифровки;
- файлы, создаваемые отдельными программами.

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Шифрование файлов имеет следующие особенности:

- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует / расшифровывает стандартные папки только для локальных профилей пользователей (англ. local user pro les) операционной системы. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не шифрует и не расшифровывает стандартные папки для перемещаемых профилей пользователей (англ. roaming user pro les), обязательных профилей пользователей (англ. mandatory user pro les), временных профилей пользователей (англ. temporary user pro les), а также перенаправленные папки.
- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не выполняет шифрование файлов, изменение которых может повредить работе операционной системы и установленных программ. Например, в список исключений из шифрования входят следующие файлы и папки со всеми вложенными в них папками:
  - %WINDIR%;
  - %PROGRAMFILES% и %PROGRAMFILES(X86)%;
  - файлы реестра Windows.

  Список исключений из шифрования недоступен для просмотра и изменения. Файлы и папки из списка исключений из шифрования можно добавить в список для шифрования, но при выполнении шифрования файлов они не будут зашифрованы.

Параметры компонента Шифрование файлов

Параметр	Описание
Управление шифрованием	Оставлять без изменений. Если выбран этот элемент, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready оставляет файлы и папки в том же состоянии – не шифрует и не расшифровывает их. Шифровать согласно правилам. Если выбран этот элемент, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует файлы и папки согласно правилам шифрования, расшифровывает файлы и папки согласно правилам расшифровки, а также регулирует доступ программ к зашифрованным файлам согласно правилам для программ. Расшифровывать все. Если выбран этот элемент, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready расшифровывает все зашифрованные файлы и папки.

Правила шифрования	На закладке отображаются правила шифрования файлов, хранящихся на локальных дисках. Вы можете добавить файлы следующим образом: • Стандартные области. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет добавить следующие области: Документы. Файлы в стандартной папке операционной системы Документы, а также вложенные папки. Избранное. Файлы в стандартной папке операционной системы Избранное, а также вложенные папки. Рабочий стол. Файлы в стандартной папке операционной системы Рабочий стол, а также вложенные папки. Временные файлы. Временные файлы, связанные с работой установленных на компьютере программ. Например, программы Microsoft O ice создают временные файлы с резервными копиями документов. Файлы Outlook. Файлы, связанные с работой почтового клиента Outlook: файлы данных (PST), автономные файлы данных (OST), файлы автономной адресной книги (OAB) и файлы персональной адресной книги (PAB). • Папки. Вы можете ввести путь к папке. При добавлении пути к папке следует использовать следующие правила: Используйте переменную окружения (например, `%FOLDER%\UserFolder\`). Вы можете использовать переменную окружения только один раз и только в начале пути. Не используйте относительные пути. Вы можете использовать набор `\..\` (например, `C:\Users\..\UserFolder\`). Набор `\..\` обозначает переход к родительской папке. Не используйте символы `*` и `?`. Не используйте UNC-пути. Используйте `;` или `,` в качестве разделительного символа. • Файлы по расширению. Вы можете выбрать группы расширений из списка, например, группу расширений Архивы. Также вы можете добавить расширение файла вручную.
Правила расшифровки	На закладке отображаются правила расшифровки файлов, хранящихся на локальных дисках.
Правила для программ	На закладке отображается таблица с правилами доступа программ к зашифрованным файлам и правилами шифрования файлов, создаваемых и изменяемых отдельными программами.
Параметры пароля для зашифрованных архивов	Параметры сложности пароля при создании зашифрованных архивов.

Шифрование съемных дисков

Этот компонент доступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready установлена на компьютере под управлением операционной системы Windows для серверов.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready поддерживает шифрование файлов в файловых системах FAT32 и NTFS. Если к компьютеру подключен съемный диск с неподдерживаемой файловой системой, то шифрование этого съемного диска завершается с ошибкой и Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready устанавливает статус доступа "только чтение" для этого съемного диска.

Для защиты данных на съемных дисках вы можете использовать следующие виды шифрования:

- Полнодисковое шифрование (англ. Full Disk Encryption – FDE).

  Шифрование всего съемного диска, включая файловую систему.

  Получить доступ к зашифрованным данным вне корпоративной сети невозможно. Также невозможно получить доступ к зашифрованным данным внутри корпоративной сети, если компьютер не подключен к Kaspersky Security Center ("гостевой" компьютер).

- Шифрование файлов (англ. File Level Encryption – FLE).

  Шифрование только файлов на съемном диске. Файловая система при этом остается без изменений.

  Шифрование файлов на съемных дисках предоставляет возможность доступа к данным за пределами корпоративной сети с помощью специального режима – портативный режим.

Во время шифрования Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready создает мастер-ключ. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет мастер-ключ в следующих хранилищах:

- Kaspersky Security Center.
- Компьютер пользователя.

  Мастер-ключ зашифрован секретным ключом пользователя.

- Съемный диск.

  Мастер-ключ зашифрован открытым ключом Kaspersky Security Center.

После завершения шифрования данные на съемном диске доступны внутри корпоративной сети как при использовании обычного съемного диска без шифрования.

Получение доступа к зашифрованным данным

При подключении съемного диска с зашифрованными данными Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

1. Проверяет наличие мастер-ключа в локальном хранилище на компьютере пользователя.

   Если мастер-ключ найден, пользователь получает доступ к данным на съемном диске.

   Если мастер-ключ не найден, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет следующие действия:

   a. Отправляет запрос в Kaspersky Security Center.

После получения запроса Kaspersky Security Center отправляет ответ, который содержит мастерключ.

b. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready сохраняет мастер-ключ в локальном хранилище на компьютере пользователя для дальнейшей работы с зашифрованным съемным диском.

2. Расшифровывает данные.

Особенности шифрования съемных дисков

Шифрование съемных дисков имеет следующие особенности:

- Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы управляемых компьютеров. Поэтому результат применения политики Kaspersky Security Center с настроенным шифрованием / расшифровкой съемных дисков зависит от того, к какому компьютеру подключен съемный диск.

- Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не выполняет шифрование / расшифровку файлов со статусом доступа "только чтение", хранящихся на съемных дисках.

- В качестве съемных дисков поддерживаются следующие типы устройств:

  - носители информации, подключаемые по шине USB;
  - жесткие диски, подключаемые по шинам USB и FireWire;
  - SSD-диски, подключаемые по шинам USB и FireWire.

Параметры компонента Шифрование съемных дисков

Параметр	Описание

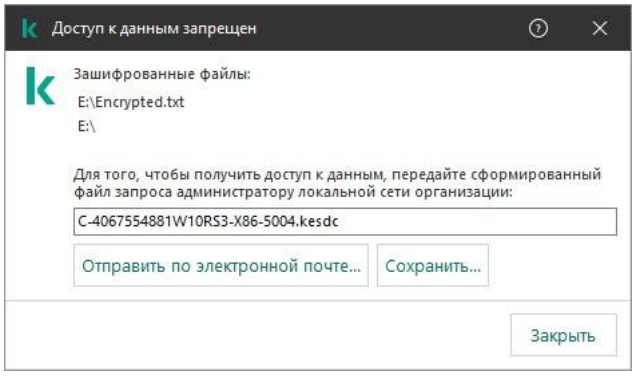
Управление шифрованием	Шифровать весь съемный диск. Если выбран этот элемент, то при применении политики с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready шифрует съемные диски по секторам, включая их файловые системы. Шифровать все файлы. Если выбран этот элемент, то при применении политики с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready шифрует все файлы, которые хранятся на съемных дисках. Уже зашифрованные файлы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready повторно не шифрует. Содержимое файловой системы съемных дисков, включая имена зашифрованных файлов и структуру папок, остается доступным и не шифруется. Шифровать только новые файлы. Если выбран этот элемент, то при применении политики с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready шифрует на съемных дисках только те файлы, которые были добавлены или изменены после последнего применения политики Kaspersky Security Center. Этот режим шифрования может быть удобным, если пользователь использует съемный диск и в личных целях, и на работе. Режим шифрования позволяет оставлять без изменений все старые файлы и шифровать только те файлы, которые пользователь создает на рабочем компьютере с установленной программой Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и доступной функциональностью шифрования. Таким образом, доступ к личным файлам всегда открыт вне зависимости от того, установлена на компьютере программа Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready с доступной функциональностью шифрования или нет. Расшифровывать весь съемный диск. Если выбран этот элемент, то при применении политики с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready расшифровывает все зашифрованные файлы, которые хранятся на съемных дисках, а также файловые системы съемных дисков, если они были зашифрованы. Оставлять без изменений. Если выбран этот элемент, то при применении политики программа оставляет диски в прежнем состоянии. Если диск был зашифрован, то он остается зашифрованным, а если диск был расшифрован, то он остается расшифрованным. Этот элемент выбран по умолчанию.
Портативный режим	Флажок включает / выключает подготовку съемного диска, которая позволяет работать с хранящимися на этом съемном диске файлами на компьютерах вне корпоративной сети. Если флажок установлен, то при применении политики перед началом шифрования файлов на съемном диске Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready запрашивает у пользователя пароль. Пароль требуется для получения доступа к зашифрованным файлам на съемном диске на компьютерах вне корпоративной сети. Вы можете настроить сложность пароля. Портативный режим доступен для режимов Шифровать все файлы или Шифровать только новые файлы.

Шифровать только занятое пространство	Флажок включает / выключает режим шифрования, при котором шифруются только занятые секторы диска. Этот режим рекомендуется применять для новых дисков, данные которых не редактировались и не удалялись. Если флажок установлен, то шифруется только та часть диска, которая занята файлами. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь диск, в том числе остатки удаленных и отредактированных ранее файлов. Функция шифрования только занятого пространства доступна только для режима Шифровать весь съемный диск. Включение / выключение функции Шифровать только занятое пространство после запуска шифрования не изменяет этого параметра. Требуется установить или снять флажок до начала шифрования.
Правила шифрования выбранных устройств	Таблица устройств, для которых заданы отдельные правила шифрования. Вы можете создать правила шифрования для отдельных съемных дисков следующими способами: • Добавьте съемный диск из списка доверенных устройств Контроля устройств. • Добавьте съемный диск вручную: • по идентификатору устройства (англ. Hardware ID – HWID); • по модели устройства: идентификатор производителя (англ. Vendor ID – VID) и идентификатор продукта (англ. Product ID – PID).
Разрешить шифрование съемных дисков в офлайнрежиме	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready шифрует съемные диски даже при отсутствии связи с Kaspersky Security Center. Данные, необходимые для расшифровки съемных дисков, сохраняются при этом на жестком диске компьютера, к которому подключен съемный диск, и не передаются на Kaspersky Security Center. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не шифрует съемные диски, если связь с Kaspersky Security Center отсутствует.
Параметры пароля для портативного режима	Параметры надежности пароля для портативного файлового менеджера.

Шаблоны (шифрование данных)

После шифрования данных Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может запретить доступ к данным, например, из-за изменения инфраструктуры организации и смены Сервера администрирования Kaspersky Security Center. Если у пользователя нет доступа к зашифрованным данным, пользователь может запросить доступ к данным у администратора. Т.е. пользователю нужно передать файл запроса администратору. Далее пользователю нужно загрузить в Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready файл ответа, полученный от администратора. Kaspersky

Endpoint Security для бизнеса - Расширенный EDR Ready позволяет запросить доступ к данным у администратора с помощью электронной почты (см. рис. ниже).



Запрос доступа к зашифрованным данным

Для сообщения об отсутствии доступа к зашифрованным данным предусмотрен шаблон. Для удобства пользователей вы можете заполнить следующие поля:

- Кому. Введите адрес электронной почты группы администраторов с правами на функции шифрования данных.
- Тема. Введите тему письма с запросом доступа к зашифрованным файлам. Вы можете, например, добавить теги для фильтрации сообщений.
- Сообщение. Если требуется измените содержание сообщения. Вы можете использовать переменные, чтобы получить необходимые данные (например, переменная %USER_NAME%).

Endpoint Sensor

В Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready 11.4.0 компонент Endpoint Sensor исключен из программы.

Вы можете управлять Endpoint Sensor в Kaspersky Security Center 12 Web Console и Консоли администрирования Kaspersky Security Center. Управлять Endpoint Sensor в программе Kaspersky Security Center Cloud Console невозможно.

Endpoint Sensor предназначен для взаимодействия с Kaspersky Anti Targeted Attack Platform. Kaspersky Anti Targeted Attack Platform – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. APT – Advanced Persistent Threat), атаки
"нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя два функциональных блока: Kaspersky Anti Targeted Attack (далее также "KATA") и Kaspersky Endpoint Detection and Response (далее также "KEDR"). Вы можете приобрести KEDR отдельно. Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Управление Endpoint Sensor имеет следующие особенности:

- Если на компьютере установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready версий 11.0.0 – 11.3.0, вы можете настроить параметры Endpoint Sensor с помощью политики. Подробнее о настройке параметров Endpoint Sensor с помощью политики см. в справке Kaspersky Endpoint Security предыдущих версий.

- Если на компьютере установлена программа Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready версии 11.4.0 и выше, настроить параметры Endpoint Sensor с помощью политики невозможно.

Endpoint Sensor устанавливается на клиентских компьютерах. На этих компьютерах компонент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Endpoint Sensor передает информацию на сервер KATA.

Функциональность компонента доступна для следующих операционных систем:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-разрядная);
- Windows Server 2012 Foundation / Standard / Enterprise (64-разрядная);
  Windows Server 2012 R2 Foundation / Standard / Enterprise (64-разрядная);
- Windows Server 2016 Essentials / Standard (64-разрядная).
-

Подробную информацию о работе KATA см. в справке Kaspersky Anti Targeted Attack Platform.

Управление задачами

Для работы с Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного клиентского компьютера; групповые задачи,
- определенные для клиентских компьютеров, входящих в группы администрирования; задачи для
- выборки компьютеров.

Вы можете создавать любое количество групповых задач, задач для выборки компьютеров и локальных задач. Подробнее о работе с группами администрирования и выборками компьютеров см. в справке Kaspersky Security Center.

Параметры управления задачами

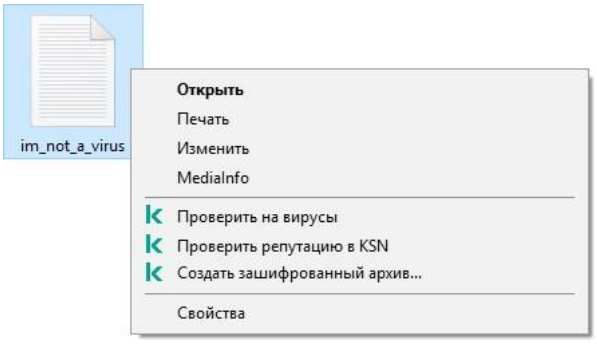
Параметр	Описание

Разрешить использование локальных задач	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Пользователь, при отсутствии дополнительных ограничений политики, может настраивать и запускать задачи. Если флажок снят, то использование локальных задач прекращается. В этом режиме локальные задачи не запускаются по расписанию. Задачи недоступны для запуска и настройки в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, а также при работе с командной строкой. Пользователь по-прежнему может запустить антивирусную проверку файла или папки, выбрав пункт Проверить на вирусы в контекстном меню файла или папки. При этом задача проверки запустится со значениями параметров, установленными по умолчанию для задачи выборочной проверки.
Разрешить отображение групповых задач	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Пользователь может просмотреть полный список задач в интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready показывает пустой список задач.
Разрешить управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в Kaspersky Security Center групповые задачи. Пользователь может запускать и останавливать задачи в интерфейсе программы или в упрощенном интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в Kaspersky Security Center.

Проверка из контекстного меню

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready позволяет проверять отдельные файлы на вирусы и другие программы, представляющие угрозу, из контекстного меню (см. рис. ниже).

При выполнении проверки из контекстного меню Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.



Проверка из контекстного меню

Параметры задачи Проверка из контекстного меню

Параметр	Описание

Действие при обнаружении угрозы	• Лечить; удалять, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready их удаляет. • Лечить; информировать, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready добавляет информацию об обнаруженных зараженных файлах в список активных угроз. • Информировать. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready добавляет информацию об этих файлах в список активных угроз.
Проверять только новые и измененные файлы	Флажок включает / выключает режим проверки только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки.
Пропускать файлы, если их проверка длится более N сек	Флажок включает / выключает ограничение длительности проверки одного объекта. По истечении заданного времени Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready прекращает проверку файла. Это позволит сократить время выполнения проверки.
Проверять архивы	Флажок включает / выключает проверку архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов.
Проверять файлы офисных форматов	Флажок включает / выключает проверку файлов Microsoft O ice (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
Не распаковывать составные файлы большого размера	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready не проверяет составные файлы, размеры которых превышают заданное значение.

Проверка съемных дисков

Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready позволяет проверять на вирусы и другие программы, представляющие угрозу, съемные диски при их подключении к компьютеру.

Параметры задачи Проверка съемных дисков

Параметр	Описание

Действие при подключении съемного диска	• Не проверять. • Подробная проверка. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет все файлы, расположенные на съемном диске, в том числе вложенные файлы внутри составных объектов. • Быстрая проверка. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет только файлы определенных форматов, наиболее подверженные заражению, а также не распаковывает составные объекты.
Максимальный размер съемного диска	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет действие, выбранное в раскрывающемся списке Действие при подключении съемного диска, над съемными дисками, размер которых не превышает указанный максимальный размер. Если флажок снят, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет действие, выбранное в раскрывающемся списке Действие при подключении съемного диска, над съемными дисками любого размера.
Отображать ход проверки	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображает ход проверки съемных дисков в отдельном окне, а также в окне Задачи. Если флажок снят, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет проверку съемных дисков в фоновом режиме.
Запретить остановку задачи проверки	Если флажок установлен, то в локальном интерфейсе Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready для задачи проверки съемных дисков недоступны кнопка Остановить в окне Задачи и кнопка Остановить в окне Антивирусная проверка.

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет объекты автозапуска, памяти ядра и системного раздела. Фоновая проверка запускается в следующих случаях:

- после обновления антивирусных баз; через 30 минут
- после запуска Kaspersky Endpoint Security для бизнеса -
- Расширенный EDR Ready; каждые шесть часов; при
- простое компьютера в течение пяти и более минут.

Фоновая проверка при простое компьютера прерывается при выполнении любого из следующих условий:

- Компьютер перешел в активный режим.

Если фоновая проверка не выполнялась более десяти дней, проверка не прерывается.

- Компьютер (ноутбук) перешел в режим питания от батареи.

При выполнении фоновой проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

Параметры программы

Вы можете настроить следующие общие параметры программы:

- режим работы; самозащита;
- производительность; отладочная информация;
- статус компьютера при применении
- параметров.

- Параметры программы

Параметр	Описание
Запускать Kaspersky Endpoint Security для Windows при включении компьютера	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready запускается после загрузки операционной системы и защищает компьютер пользователя в течение всего сеанса работы. Если флажок не установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не запускается после загрузки операционной системы до того момента, как пользователь запустит программу вручную. Защита компьютера выключена и данные пользователя могут находиться под угрозой.
Применять технологию лечения активного заражения	Если флажок установлен, при обнаружении вредоносной активности в операционной системе на экране отображается всплывающее уведомление. В уведомлении Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предлагает провести процедуру лечения активного заражения компьютера. После подтверждения пользователем этой процедуры Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready устраняет угрозу. Завершив процедуру лечения активного заражения, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет перезагрузку компьютера. Применение технологии лечения активного заражения требует значительных ресурсов компьютера, что может замедлить работу других программ. Технология лечения активного заражения доступна только на компьютерах под управлением операционной системы Windows для рабочих станций. Использовать технологию лечения активного заражения на компьютерах под управлением операционной системы Windows для серверов невозможно.

Использовать Kaspersky Security Center в качестве прокси-сервера для активации	Если флажок установлен, то при активации программы в качестве прокси-сервера используется Сервер администрирования Kaspersky Security Center.
Включить самозащиту	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти и записей в системном реестре.
Выключить внешнее управление системными службами	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует все попытки управления службами программы с удаленного компьютера. При попытке управления службами программы с удаленного компьютера, над значком программы в области уведомлений панели задач Microsoft Windows отображается уведомление (если служба уведомлений не выключена пользователем).
Откладывать задачи по расписанию при работе от аккумулятора	Если флажок установлен, то режим экономии питания аккумулятора включен. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready откладывает выполнение задач, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления.
Уступать ресурсы другим программам	Когда Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выполняет задачи по расписанию, может увеличиваться нагрузка на центральный процессор и дисковые подсистемы, что замедляет работу других программ. Если флажок установлен, то при увеличении нагрузки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready приостанавливает выполнение задач по расписанию и высвобождает ресурсы операционной системы для других программ.
Включить запись дампов	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready записывает дампы в случае сбоев в работе. Если флажок снят, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не записывает дампы. Программа удаляет уже существующие на жестком диске компьютера файлы дампов.
Включить защиту файлов дампов и файлов трассировки	Если флажок установлен, то доступ к файлам дампов предоставляется системному и локальному администраторам, а также пользователю, включившему запись дампов. Доступ к файлам трассировки предоставляется только системному и локальному администраторам. Если флажок снят, доступ к файлам дампов и файлам трассировки имеет любой пользователь.
Статус компьютера при применении параметров	Параметры отображения статусов клиентских компьютеров с установленной программой Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в Web Console при появлении ошибок применения политики или выполнения задачи. Доступны статусы OK, Предупреждение и Критический.

Параметры сети

Вы можете настроить параметры прокси-сервера для подключения к интернету и обновления антивирусных баз, выбрать режим контроля сетевых портов и настроить проверку защищенных соединений.

Параметры сети

Параметр	Описание
Параметры прокси-сервера	Параметры прокси-сервера для доступа пользователей клиентских компьютеров в интернет. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей программы. Для автоматической настройки прокси-сервера Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует протокол WPAD (Web Proxy Auto-Discovery Protocol). В случае если по этому протоколу не удается определить IP-адрес прокси-сервера, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready использует адрес прокси-сервера, указанный в параметрах браузера Microsoft Internet Explorer.
Не использовать прокси-сервер для локальных адресов	Если флажок установлен, то при обновлении Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready из папки общего доступа прокси-сервер не используется.
Контролируемые порты	• Контролировать все сетевые порты. Режим контроля сетевых портов, при котором компоненты защиты (Защита от файловых угроз, Защита от веб-угроз, Защита от почтовых угроз) контролируют потоки данных, передаваемые через любые открытые сетевые порты компьютера. • Контролировать только выбранные сетевые порты. Режим контроля сетевых портов, при котором компоненты защиты контролируют выбранные пользователем сетевые порты компьютера. Список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика, настроен в соответствии с рекомендациями специалистов "Лаборатории Касперского".
Проверять защищенные соединения	Если флажок установлен, компоненты Защита от веб-угроз, Защита от почтовых угроз и Веб-Контроль проверяют зашифрованный сетевой трафик, передаваемый по следующим протоколам: • SSL 3.0; • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет защищенные соединения, установленные программами, для которых установлен флажок Не проверять сетевой трафик в окне Исключения из проверки для программы.

При переходе на домен с недоверенным сертификатом	• Разрешать. Если выбран этот вариант, то при переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready разрешает установку сетевого соединения. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения. По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу. После перехода по этой ссылке Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready в течение часа не будет отображать предупреждения о недоверенном сертификате при переходе на другие веб-ресурсы в том же домене. • Блокировать соединение. Если выбран этот вариант, то при переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует сетевое соединение. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отображает HTML-страницу с информацией о причине, по которой переход на этот домен заблокирован.
При возникновении ошибок проверки защищенных соединений	• Блокировать соединение. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует это сетевое соединение. • Добавлять домен в исключения. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready добавляет домен, при переходе на который возникла ошибка, в список доменов с ошибками проверки и не контролирует зашифрованный сетевой трафик при переходе на этот домен. Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе программы. Чтобы сбросить содержание списка, нужно выбрать элемент Блокировать соединение.
Блокировать соединения по протоколу SSL 2.0	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0, и не контролирует сетевой трафик, передаваемый по этим соединениям.

Расшифровать защищенное соединение с сайтом, использующим EV-сертификат	EV-сертификаты (англ. Extended Validation Certi cate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет. Если флажок установлен, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не имеет доступа к содержанию HTTPS-трафика. Поэтому программа контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://facebook.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.
Доверенные адреса	Список веб-адресов, для которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет защищенные сетевые соединения.
Доверенные программы	Список программ, активность которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет в процессе своей работы. Вы можете выбрать виды активности программы, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не будет контролировать (например, не проверять сетевой трафик).

Исключения

Доверенная зона – это сформированный администратором системы список объектов и программ, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не контролирует в процессе работы. Иначе говоря, это набор исключений из проверки.

Доверенную зону администратор системы формирует самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от программ, установленных на компьютере. Включение объектов и программ в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что этот объект или программа безвредны.

Вы можете исключать из проверки объекты следующими способами:

- укажите путь к файлу или папке;
- введите хеш объекта;
- используйте маски:
  - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске C, но не в подпапках.
  - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам).

Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папке `Folder` и вложенных папках. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

- введите название объекта по классификации Вирусной энциклопедии "Лаборатории Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

Исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет объект на вирусы и другие программы, представляющие угрозу.

Исключения из проверки позволяют работать с легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского".

В результате работы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready такие программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ вы можете настроить исключения из проверки. Для этого нужно добавить в доверенную зону название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского". Например, вы часто используете в своей работе программу Radmin, предназначенную для удаленного управления компьютерами. Такая активность программы рассматривается Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready как подозрительная и может быть заблокирована. Чтобы исключить блокировку программы, нужно сформировать исключение из проверки, где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

Если у вас на компьютере установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из проверки, настроив Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready способом, описанным в этом документе.

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач программы, заданных администратором системы:

- Анализ поведения.
- Защита от эксплойтов.
- Предотвращение вторжений.
- Защита от файловых угроз.
- Защита от веб-угроз.

- Защита от почтовых угроз.
- Задачи проверки.

Список доверенных программ

Список доверенных программ – это список программ, у которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не контролирует файловую и сетевую активность (в том числе и вредоносную), а также обращения этих программ к системному реестру. По умолчанию Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready исключает из проверки программу, добавленную в список доверенных программ.

Например, если вы считаете объекты, используемые программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, вам следует добавить программу Microsoft Windows Блокнот в список доверенных программ, чтобы не проверять объекты, используемые этой программой.

Кроме того, некоторые действия, которые Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда программ. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных программ.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready и другой антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

В то же время исполняемый файл и процесс доверенной программы по-прежнему проверяются на наличие в них вирусов и других программ, представляющих угрозу. Для полного исключения программы из проверки Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready следует пользоваться исключениями из проверки.

Параметры исключений

Параметр	Описание

Объекты для обнаружения	Вне зависимости от настроенных параметров программы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready всегда обнаруживает и блокирует вирусы, черви и троянские программы. Эти программы могут нанести значительный вред компьютеру. • Вирусы, черви

Подкатегория: вирусы и черви (Viruses_and_Worms)

Степень угрозы: высокая

Классические вирусы и черви выполняют на компьютере действия, не разрешенные пользователем. Они могут создавать свои копии, которые обладают способностью дальнейшего самовоспроизведения.

Классический вирус

Попав в систему, классический вирус заражает какой-либо файл, активизируется в нем, выполняет свое вредоносное действие, а затем добавляет свои копии в другие файлы.

Классический вирус размножается только на локальных ресурсах компьютера и не может самостоятельно проникать на другие компьютеры. Он может попасть на другой компьютер только в том случае, если добавит свою копию в файл, который хранится в папке общего доступа или на установленном компакт-диске, или если пользователь сам перешлет сообщение электронной почты с вложенным в него зараженным файлом.

Код классического вируса может внедряться в различные области компьютера, операционной системы или приложения. В зависимости от среды обитания вирусы подразделяют на файловые, загрузочные, скриптовые и макро-вирусы.

Вирусы могут заражать файлы различными способами. Перезаписывающие (Overwriting) вирусы записывают свой код вместо кода заражаемого файла, уничтожая его содержимое. Зараженный файл перестает работать, и его нельзя восстановить. Паразитические (Parasitic) вирусы изменяют файлы, оставляя их полностью или частично работоспособными. Вирусы-компаньоны (Companion) не изменяют файлы, но создают их двойники. При открытии зараженного файла запускается его двойник, то есть вирус. Среди вирусов встречаются также
вирусы-ссылки (Link), вирусы, заражающие объектные модули (OBJ), вирусы, заражающие библиотеки компиляторов (LIB), вирусы, заражающие исходные тексты программ, и другие.

Червь

Код червя, как и код классического вируса, попав в систему, активизируется и выполняет свое вредоносное действие. Свое название червь получил благодаря способности "переползать" с компьютера на компьютер – без разрешения пользователя распространять свои копии через различные информационные каналы.

Основной признак, по которому черви различаются между собой, – способ их распространения. Описание типов червей по способу распространения приводится в следующей таблице.

Способы распространения червей

Тип	Название	Описание

Email-Worm	Почтовые черви	Распространяются через электронную почту. Зараженное сообщение электронной почты содержит прикрепленный файл с копией червя или ссылку на такой файл на веб-сайте, например, взломанном или специально созданном. Когда вы запускаете прикрепленный файл, червь активизируется; когда вы щелкаете на ссылке, загружаете, а затем открываете файл, червь также начинает выполнять свое вредоносное действие. После этого он продолжает распространять свои копии, разыскивая другие адреса электронной почты и отправляя по ним зараженные сообщения.
IM-Worm	IM-клиентов	Распространяются через IM-клиенты. Обычно такой червь рассылает по контактлистам сообщения, содержащие ссылку на файл с его копией на веб-сайте. Когда пользователь загружает файл и открывает его, червь активизируется.
IRC-Worm	Черви интернет-чатов	Распространяются через ретранслируемые интернет-чаты (Internet Relay Chats) – сервисные системы, с помощью которых можно общаться через интернет с другими людьми в реальном времени. Такой червь публикует в интернет-чате файл со своей копией или ссылку на файл. Когда пользователь загружает файл и открывает его, червь активизируется.
Net-Worm	Сетевые черви (черви компьютерных сетей)	Распространяются через компьютерные сети. В отличие от червей других типов, сетевой червь распространяется без участия пользователя. Он ищет в локальной сети компьютеры, на которых используются программы, содержащие уязвимости. Для этого он посылает специально сформированный сетевой пакет (эксплойт), который содержит код червя или его часть. Если в сети находится "уязвимый" компьютер, он принимает такой сетевой пакет. Полностью проникнув на компьютер, червь активизируется.

P2P-Worm	Черви файлообменных сетей	Распространяются через файлообменные пиринговые сети. Чтобы внедриться в файлообменную сеть, червь копирует себя в каталог обмена файлами, обычно расположенный на компьютере пользователя. Файлообменная сеть отображает информацию об этом файле, и пользователь может "найти" зараженный файл в сети так же, как и любой другой, загрузить его и открыть. Более сложные черви имитируют сетевой протокол конкретной файлообменной сети: они положительно отвечают на поисковые запросы и предлагают для загрузки свои копии.
Worm	Прочие черви	К прочим сетевым червям относятся:

		• Черви, которые распространяют свои копии через сетевые ресурсы. Используя функции операционной системы, они перебирают доступные сетевые папки, подключаются к компьютерам в глобальной сети и пытаются открыть их диски на полный доступ. В отличие от описанных выше разновидностей червей, прочие черви активизируются не самостоятельно, а как только пользователь открывает файл с копией червя. • Черви, которые не относятся ни к одному из описанных в этой таблице способов распространения (например, те, которые распространяются черезмобильные телефоны).

- Троянские программы

Подкатегория: троянские программы (Trojan_programs)

Степень угрозы: высокая

В отличие от червей и вирусов, троянские программы не создают свои копии. Они проникают на компьютер, например, через электронную почту или через браузер, когда пользователь посещает зараженную веб-страницу. Троянские программы запускаются при участии пользователя. Они начинают выполнять свое вредоносное действие сразу после запуска.

Разные троянские программы ведут себя на зараженном компьютере поразному. Основные функции троянских программ – блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Кроме этого, троянские программы могут принимать или отправлять файлы, выполнять их, выводить на экран сообщения, обращаться к веб-страницам, загружать и устанавливать программы, перезагружать компьютер.

Злоумышленники часто используют "наборы" из разных троянских программ.

Типы поведения троянских программ описаны в следующей таблице.

Типы поведения троянских программ на зараженном компьютере

Тип	Название	Описание
Trojan-ArcBomb	Троянские программы – "архивные бомбы"	Архивы; при распаковке увеличиваются до таких размеров, что нарушают работу компьютера. Когда пользователь пытается распаковать такой архив, компьютер может начать работать медленно или "зависнуть", диск может заполниться "пустыми" данными. "Архивные бомбы" особенно опасны для файловых и почтовых серверов. Если на сервере используется система автоматической обработки входящей информации, такая "архивная бомба" может остановить сервер.
Backdoor	Троянские программы удаленного администрирования	Считаются наиболее опасными среди троянских программ. По своим функциям напоминают устанавливаемые на компьютеры программы удаленного администрирования. Эти программы устанавливают себя в компьютере незаметно для пользователя и позволяют злоумышленнику удаленно управлять компьютером.

Trojan	Троянские программы	Включают следующие вредоносные программы: • Классические троянские программы. Эти программы выполняют только основные функции троянских программ: блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Они не имеют дополнительных функций, свойственных другим типам троянских программ, описанным в этой таблице. • "Многоцелевые" троянские программы. Эти программы имеют дополнительные функции, присущие сразу нескольким типам троянских программ.
Trojan-Ransom	Троянские программы, требующие выкупа	"Берут в заложники" информацию на компьютере пользователя, изменяя или блокируя ее, или нарушают работу компьютера таким образом, чтобы пользователь не мог воспользоваться информацией. Злоумышленник требует от пользователя выкуп за обещание выслать программу, которая восстановит работоспособность компьютера и данные на нем.
Trojan-Clicker	Троянские программы-кликеры	С компьютера пользователя обращаются к веб-страницам: они или сами посылают команды браузеру, или заменяют хранящиеся в системных файлах веб-адреса. С помощью этих программ злоумышленники организовывают сетевые атаки, повышают посещаемость сайтов, чтобы увеличить количество показов рекламных баннеров.

Trojan-Downloader	Троянские программызагрузчики	Обращаются к веб-странице злоумышленника, загружают с нее другие вредоносные программы и устанавливают их на компьютере пользователя; могут хранить имя файла загружаемой вредоносной программы в себе или получать его с вебстраницы, к которой обращаются.
Trojan-Dropper	Троянские программыустановщики	Сохраняют на диске компьютера, а затем устанавливают другие троянские программы, которые хранятся в теле этих программ. Злоумышленники могут использовать троянские программы-установщики, чтобы достичь следующих целей: • установить вредоносную программу незаметно для пользователя: троянские программы-установщики не отображают никаких сообщений или выводят на экран ложные сообщения, например, об ошибке в архиве или неверной версии операционной системы; • защитить от обнаружения другую известную вредоносную программу: не все антивирусы могут распознать вредоносную программу внутри троянской программы-установщика.
Trojan-Noti er	Троянские программыуведомители	Сообщают злоумышленнику о том, что зараженный компьютер находится "на связи"; передают ему информацию о компьютере: IP-адрес, номер открытого порта или адрес электронной почты. Они связываются со злоумышленником по электронной почте, через FTP, обращаясь к его вебстранице или другим способом. Троянские программы-уведомители часто используются в наборах из разных троянских программ. Они извещают злоумышленника о том, что другие троянские программы успешно установлены на компьютере пользователя.

Trojan-Proxy	Троянские программы-прокси	Позволяют злоумышленнику анонимно обращаться через компьютер пользователя к веб-страницам; часто используются для рассылки спама.
Trojan-PSW	Троянские программы, крадущие пароли	Троянские программы, крадущие пароли (Password Stealing Ware); крадут учетные записи пользователей, например, регистрационную информацию к программному обеспечению. Они отыскивают конфиденциальные данные в системных файлах и реестре и пересылают ее "хозяину" по электронной почте, через FTP, обращаясь к веб-странице злоумышленника или другим способом. Некоторые из этих троянских программ выделены в отдельные типы, описанные в этой таблице. Это троянские программы, крадущие банковские счета (Trojan-Banker), троянские программы, крадущие данные пользователей IM-клиентов (Trojan-IM) и троянские программы, крадущие данные пользователей сетевых игр (Trojan-GameThief).
Trojan-Spy	Троянские программы-шпионы	Ведут электронный шпионаж за пользователем: собирают информацию о его действиях на компьютере, например, перехватывают данные, которые пользователь вводит с клавиатуры, делают снимки экрана или собирают списки активных приложений. Получив эту информацию, они передают ее злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.

Trojan-DDoS	Троянские программы – сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании). Такими программами часто заражают многие компьютеры, чтобы с них одновременно атаковать один сервер. DoS-программы реализуют атаку с одного компьютера с ведома пользователя. DDoS-программы (Distributed DoS) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователя зараженного компьютера.
Trojan-IM	Троянские программы, крадущие данные пользователей IMклиентов	Крадут номера и пароли пользователей IM-клиентов. Передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его вебстранице или другим способом.
Rootkit	Руткиты	Скрывают другие вредоносные программы и их активность и таким образом продлевают пребывание этих программ в системе; могут скрывать файлы, процессы в памяти зараженного компьютера или ключи реестра, которые запускают вредоносные программы; могут скрывать обмен данными между приложениями на компьютере пользователя и других компьютерах в сети.
Trojan-SMS	Троянские программы – SMScообщения	Заражают мобильные телефоны и с них отправляют SMS-сообщения на платные номера.
Trojan-GameThief	Троянские программы, крадущие данные пользователей сетевых игр	Крадут учетные данные пользователей сетевых компьютерных игр; передают их злоумышленнику по электронной почте, через FTP, обращаясь к его вебстранице или другим способом.
Trojan-Banker	Троянские программы, крадущие банковские счета	Крадут данные банковских счетов или счетов в системах электронных денег; передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.

Trojan-Mail nder	Троянские программы – сборщики адресов электронной почты	Собирают адреса электронной почты на компьютере и передают их злоумышленнику по электронной почте, через FTP, обращаясь к его вебстранице или другим способом. По собранным адресам злоумышленники могут рассылать спам.

Вредоносные утилиты

Подкатегория: вредоносные утилиты (Malicious_tools)

Уровень опасности: средний

Вредоносные утилиты, в отличие от других вредоносных программ, не выполняют своих действий сразу при запуске и могут безопасно храниться и запускаться на компьютере пользователя. Злоумышленники используют функции этих программ для создания вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы, "взлома" компьютеров или других вредоносных действий.

Разнообразные функции вредоносных утилит делятся на типы, которые описаны в следующей таблице.

Функции вредоносных утилит

Тип	Название	Описание
Constructor	Конструкторы	Позволяют создавать новые вирусы, черви и троянские программы. Некоторые конструкторы имеют стандартный оконный интерфейс, в котором с помощью меню можно выбирать тип создаваемой вредоносной программы, способ ее противодействия отладчику и другие свойства.
Dos	Сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании).

Exploit	Эксплойты	Эксплойт – это набор данных или программный код, использующий уязвимости приложения, в котором он обрабатывается, чтобы выполнить на компьютере вредоносное действие. Например, эксплойт может записывать или считывать файлы либо обращаться к "зараженным" веб-страницам.
		Разные эксплойты используют уязвимости разных приложений или сетевых служб. Эксплойт в виде сетевого пакета передается по сети на многие компьютеры, выискивая компьютеры с уязвимыми сетевыми службами. Эксплойт в файле DOC использует уязвимости текстового редактора. Он может начать выполнять заложенные в него злоумышленником функции, когда пользователь откроет зараженный файл. Эксплойт, внедренный в сообщение электронной почты, ищет уязвимости в каком-либо почтовом клиенте. Он может начать выполнять вредоносное действие, как только пользователь откроет зараженное сообщение в этом почтовом клиенте. С помощью эксплойтов распространяются сетевые черви (NetWorm). Эксплойты-ньюкеры (Nuker) представляют собой сетевые пакеты, которые выводят компьютеры из строя.
FileCryptor	Шифровальщики	Шифруют другие вредоносные программы, чтобы скрыть их от антивирусного приложения.

Flooder	Программы для "замусоривания" сетей	Рассылают многочисленные сообщения по сетевым каналам. К этому типу относятся, например, программы для замусоривания ретранслируемых интернет-чатов (Internet Relay Chats). К типу Flooder не относятся программы, "забивающие мусором" каналы электронной почты, IM-клиентов и мобильных систем. Эти программы выделяют в отдельные типы, описанные в этой таблице (Email-Flooder, IM-Flooder и SMS-Flooder).
HackTool	Инструменты хакера	Позволяют взламывать компьютер, на котором они установлены, или атаковать другой компьютер (например, без разрешения пользователя добавлять других пользователей системы; очищать системные журналы, чтобы скрыть следы присутствия в системе). К этому типу относят некоторые снифферы, которые обладают вредоносными функциями, например перехватывают пароли. Снифферы (Sni ers) – это программы, которые позволяют просматривать сетевой трафик.
Hoax	Злые шутки	Пугают пользователя вирусоподобными сообщениями: могут "обнаружить" вирус в незараженном файле или объявить о форматировании диска, которого на самом деле не происходит.

Spoofer	Утилитыимитаторы	Отправляют сообщения и сетевые запросы с поддельным адресом отправителя. Злоумышленники используют утилиты-имитаторы, чтобы, например, выдать себя за отправителя.
VirTool	Инструменты для модификации вредоносных программ	Позволяют модифицировать другие вредоносные программы так, чтобы скрыть их от антивирусных приложений.
Email-Flooder	Программы для "замусоривания" адресов электронной почты	Отправляют многочисленные сообщения по адресам электронной почты ("забивают их мусором"). Большой поток сообщений не дает пользователям просматривать полезную входящую почту.
IM-Flooder	Программы для "замусоривания" IM-клиентов	Отправляют многочисленные сообщения пользователям IM-клиентов. Большой поток сообщений не дает пользователям просматривать полезные входящие сообщения.
SMS-Flooder	Программы для "замусоривания" SMSсообщениями	Отправляют многочисленные SMSсообщения на мобильные телефоны.

Подкатегория: рекламные программы (Adware)

Степень угрозы: средняя

Рекламные программы связаны с показом пользователю рекламной информации. Они отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-страницы. Некоторые из них собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов, рекламные программы передают эту информацию разработчику с разрешения пользователя.

Рекламные программы

Программы автодозвона

Подкатегория: легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Уровень опасности: средний

Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Однако если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые их функции для нарушения безопасности.

Подобные программы различают по функциям, типы которых описаны в таблице ниже.

Тип	Название	Описание
Client-IRC	Клиенты интернетчатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
Downloader	Программызагрузчики	Могут загружать файлы с вебстраниц в скрытом режиме.
Monitor	Программымониторы	Позволяют наблюдать за активностью на компьютере, на котором установлены (видеть, какие приложения работают, и как они обмениваются данными с приложениями на других компьютерах).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники.

RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры пользователей для наблюдения за удаленными компьютерами и управления ими.

		Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на локальном компьютере	Дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы).

NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

-

Другие

Подкатегория: легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Уровень опасности: средний

Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Однако если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые их функции для нарушения безопасности.

Подобные программы различают по функциям, типы которых описаны в таблице ниже.

Тип	Название	Описание
Client-IRC	Клиенты интернетчатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
Downloader	Программызагрузчики	Могут загружать файлы с вебстраниц в скрытом режиме.
Monitor	Программымониторы	Позволяют наблюдать за активностью на компьютере, на котором установлены (видеть, какие приложения работают, и как они обмениваются данными с приложениями на других компьютерах).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники.

RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры пользователей для наблюдения за удаленными компьютерами и управления ими.
		Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на локальном компьютере	Дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы).

		для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет упакованные объекты и модульраспаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive).

Чтобы скрыть опасные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков или многократно упаковывают один объект.

Вирусные аналитики "Лаборатории Касперского" отобрали упаковщики, которые злоумышленники используют чаще всего.

Если Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обнаружил в объекте такой упаковщик, то скорее всего он содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выделяет следующие программы:

- Упакованные файлы, которые могут нанести вред – используются для упаковки вредоносных программ: вирусов, червей, троянских программ.
- Многократно упакованные файлы (степень угрозы средняя) – объект упакован трижды одним или несколькими упаковщиками.

Упакованные файлы, которые могут нанести вред

Многократно упакованные файлы

	Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready проверяет упакованные объекты и модульраспаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive). Чтобы скрыть опасные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков или многократно упаковывают один объект. Вирусные аналитики "Лаборатории Касперского" отобрали упаковщики, которые злоумышленники используют чаще всего. Если Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready обнаружил в объекте такой упаковщик, то скорее всего он содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя. Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready выделяет следующие программы: • Упакованные файлы, которые могут нанести вред – используются для упаковки вредоносных программ: вирусов, червей, троянских программ. • Многократно упакованные файлы (степень угрозы средняя) – объект упакован трижды одним или несколькими упаковщиками.
Исключения	Таблица содержит информацию об исключениях из проверки.

из проверки	Вы можете исключать из проверки объекты следующими способами: • укажите путь к файлу или • папке; введите хеш объекта; • используйте маски: • Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске C, но не в подпапках. • Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папке `Folder` и вложенных папках. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. • Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем файлам с расширением txt и именем, состоящим из трех символов, расположенным в папке `Folder`. • введите название объекта по классификации Вирусной энциклопедии "Лаборатории Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).
Доверенные программы	Таблица доверенных программ, активность которых Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready не проверяет в процессе своей работы. Компонент Контроль программ регулирует запуск каждой из программ независимо от того, указана ли эта программа в таблице доверенных программ или нет.
Использовать доверенное системное хранилище сертификатов	Если флажок установлен, то Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready исключает из проверки программы, подписанные доверенной цифровой подписью. Компонент Предотвращение вторжений автоматически помещает такие программы в группу Доверенные. Если флажок снят, то антивирусная проверка выполняется независимо от наличия у программы цифровой подписи. Компонент Предотвращение вторжений распределяет программы по группам доверия согласно установленным параметрам.

Отчеты и хранение

Отчеты

Информация о работе каждого компонента Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready, о событиях шифрования данных, о выполнении каждой задачи проверки, задачи обновления и задачи проверки целостности, а также о работе программы в целом сохраняется в отчетах.

Отчеты хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\Report`.

Резервное хранилище

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. Резервная копия – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

В Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Параметры отчетов и хранения

Параметр	Описание
Хранить отчеты не более N дней	Если флажок установлен, то максимальный срок хранения отчетов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения отчетов составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически удаляет наиболее старые записи из файла отчета.
Максимальный размер файла N МБ	Если флажок установлен, то максимальный размер файла отчета ограничен заданным значением. По умолчанию максимальный размер файла составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически удаляет наиболее старые записи из файла отчета таким образом, чтобы размер файла отчета не превышал максимального значения.
Хранить объекты не более N дней	Если флажок установлен, то максимальный срок хранения файлов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения файлов составляет 30 дней. По истечении максимального срока хранения Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready удаляет наиболее старые файлы из резервного хранилища.
Максимальный размер хранилища N МБ	Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию максимальный размер составляет 100 МБ. После достижения максимального размера резервного хранилища Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.
Передача данных на Сервер администрирования	Категории событий на клиентских компьютерах, информация о которых должна передаваться на Сервер администрирования.

Интерфейс

Вы можете настроить параметры интерфейса программы.

Параметры интерфейса

Параметр	Описание
Взаимодействие с пользователем	• С упрощенным интерфейсом. На клиентском компьютере недоступно главное окно программы, а доступен только значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Также Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready показывает уведомления над значком программы. • С полным интерфейсом. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready и значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Также Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready показывает уведомления над значком программы. • Без интерфейса. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready. Также недоступны значок в области уведомлений Windows и уведомления.
Уведомления	• Правила уведомлений. Таблица с параметрами уведомлений о событиях различного уровня важности, которые могут происходить во время работы компонента или программы в целом, а также выполнения задачи. Уведомления об этих событиях Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready выводит на экран, доставляет по электронной почте или сохраняет в журналы. • Настройка почтовых уведомлений. Параметры SMTP-сервера для рассылки оповещений о событиях, регистрируемых при работе программы.
Предупреждения	Категории событий программы, при возникновении которых меняется значок Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready в области уведомлений панели задач Microsoft Windows (или).
Уведомления о состоянии локальных антивирусных баз	Параметры уведомлений о неактуальности антивирусных баз, которые использует программа.
Защита паролем	Если переключатель включен, Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready запрашивает пароль при попытке пользователя совершить операцию, входящую в область действия Защиты паролем. Область действия Защиты паролем включает в себя запрещенные операции (например, выключение компонентов защиты) и учетные записи пользователей, на которые распространяется область действия Защиты паролем. После включения Защиты паролем Kaspersky Endpoint Security для бизнеса – Расширенный EDR Ready предлагает задать пароль для выполнения операций.

Веб-ресурсы Службы технической поддержки	Список ссылок на веб-сайты с информацией о технической поддержке программы Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready. Добавленные ссылки отображаются в окне Поддержка локального интерфейса Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready вместо стандартных ссылок.
Сообщение пользователю	Сообщение, которое отображается в окне Поддержка локального интерфейса Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready.

Приложение 2. Группы доверия программ

Все программы, запускаемые на компьютере, Kaspersky Endpoint Security для бизнеса - Расширенный EDR Ready распределяет на группы доверия. Программы распределяются на группы доверия в зависимости от степени угрозы, которую эти программы могут представлять для операционной системы.

Существуют следующие группы доверия:

- Доверенные. В группу входят программы, для которых выполняется одно или более следующих условий:
  - Программы обладают цифровой подписью доверенных производителей.
  - О программах есть записи в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Доверенные".

  Запрещенных операций для таких программ нет.
- Слабые ограничения. В группу входят программы, для которых выполняются следующие условия:
  - Программы не обладают цифровой подписью доверенных производителей.
  - О программах нет записей в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Слабые ограничения".

  Такие программы имеют минимальные ограничения на работу с ресурсами операционной системы.
- Сильные ограничения. В группу входят программы, для которых выполняются следующие условия:
  - Программы не обладают цифровой подписью доверенных производителей.
  - О программах нет записей в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Сильные ограничения".

  Такие программы имеют значительные ограничения на работу с ресурсами операционной системы.
- Недоверенные. В группу входят программы, для которых выполняются следующие условия:
  - Программы не обладают цифровой подписью доверенных производителей.
  - О программах нет записей в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Недоверенные".

Для таких программ запрещены все операции.

Приложение 3. Категории содержания веб-ресурсов

Категории содержания веб-ресурсов (далее также "категории") в приведенном ниже списке подобраны таким образом, чтобы максимально полно описать блоки информации, размещенные на веб-ресурсах, с учетом их функциональных и тематических особенностей. Порядок категорий в списке не отражает относительной важности или распространенности категорий в сети Интернет. Названия категорий являются условными и используются лишь для целей программ и веб-сайтов "Лаборатории Касперского". Названия не обязательно соответствуют значению, которое им придает применимое законодательство. Один веб-ресурс может относиться к нескольким категориям одновременно.

Для взрослых

В общем определении категория включает в себя веб-ресурсы, относящиеся к сексуальной стороне человеческих отношений, философий, секс магазинов и т.д. Это может быть содержимое в любом формате и виде.

Алкоголь, табак, наркотики и психотропы

В общем определении категория включает в себя веб ресурсы, на которых есть упоминание алкоголя, наркотиков, табака в любых видах, в том числе рекламные, исторические, медицинские и обучающие ресурсы. А также веб ресурсы, где описаны или продаются приспособления для употребления указанных веществ.

Насилие

Данная категория включает веб-ресурсы, содержащие фото-, видео- и текстовые материалы, описывающие акты физического или психического насилия над людьми, а также жестокого отношения к животным как цель существования этого контента.

> Произведения искусства могут быть исключениями в этой категории.

Нецензурная лексика

Категория включает веб-ресурсы, на которых обнаружены элементы нецензурной брани.

> В данную категорию так же попадают веб-ресурсы с лингвистическими и филологическими материалами, содержащими нецензурную лексику в качестве предмета рассмотрения.

Оружие, взрывчатые вещества, пиротехника

Данная категория включает веб-ресурсы, содержащие информацию об оружии, взрывчатых веществах и пиротехнической продукции.

> Под "оружием" понимаются устройства, предметы и средства, конструктивно предназначенные для нанесения вреда жизни и здоровью людей и животных и / или выведения из строя техники и сооружений.

Поиск работы

Данная категория включает веб-ресурсы, предназначенные для установления контактов между работодателем и соискателем работы. К ним в частности относятся:

- Веб-сайты кадровых агентств (агентств по трудоустройству и/или агентств по подбору персонала).
- Веб-страницы работодателей, содержащие описание имеющихся вакансий и их преимуществ.
- Независимые порталы, содержащие предложения трудоустройства от работодателей и кадровых агентств.
- Социальные сети профессионального характера, которые в том числе позволяют размещать/находить данные о специалистах, которые не находятся в активном поиске работы.

Средства анонимного доступа

Данная категория включает веб-ресурсы, выступающие в роли посредника для загрузки контента прочих веб-ресурсов с помощью специальных веб-приложений для:

- обхода ограничений администратора локальной сети на доступ к веб-адресам или IP-адресам;
- анонимного доступа к веб-ресурсам, в том числе к веб-ресурсам, которые преднамеренно не принимают HTTP-запросы с определённых IP-адресов или их групп (например, по стране происхождения).

Программное обеспечение, аудио, видео

В общем определении категория включает в себя веб-ресурсы, предоставляющие возможность скачивания соответствующих файлов.

- Торренты

  Торрент трекеры и веб ресурсы, помогающие организовать их работу.

- Файловые обменники

  Веб-ресурсы, предоставляющие возможность обмена файлами.

- Аудио, видео

  Веб-ресурсы, с которых можно загрузить или просмотреть/прослушать аудио или видео файлы.

Азартные игры, лотереи, тотализаторы

Категория охватывает веб-ресурсы, содержащие:

- Азартные игры, предусматривающие денежные взносы за участие.
- Тотализаторы, предусматривающие денежные ставки.
- Лотереи, предусматривающие приобретение лотерейных билетов/номеров.

Общение в сети

В общем определении категория включает в себя веб-ресурсы, позволяющие тем или иным пользователям (зарегистрированным или нет) отправлять персональные сообщения другим пользователям. Существует ряд веб-ресурсов рассчитанных на общение.

- Веб-почта

  Веб-почта - исключительно страницы авторизации в почтовом сервисе и страницы почтового ящика, содержащего почтовые сообщения и сопутствующие данные (например, личные контакты). Для остальных веб-страниц интернет-провайдера, предлагающего почтовый сервис, данная категория не назначается.

- Социальные сети

  Социальные сети – веб-сайты, предназначенные для построения, отражения и организации контактов между людьми, организациями, государством, требующие в качестве условия участия регистрацию учётной записи пользователя.

- Чаты, форумы

  В данную категорию следует относить веб-чаты, а также веб-ресурсы, предназначенные для распространения и поддержки приложений для обмена мгновенными сообщениями, предоставляющих возможность коммуникации в реальном времени. А также форумы – специальные веб сервисы для публичного обсуждения различных тем с сохранением переписки.

- Блоги

  Блоги – веб-ресурсы, предназначенные для публичного обсуждения различных тем с помощью специальных веб-приложений, включая блог-платформы (веб-сайты, предоставляющие платные или бесплатные услуги по созданию и обслуживанию блогов).

- Сайты знакомств

  Веб ресурсы знакомств, которые помогают организовать знакомства между людьми, в том числе без сексуального подтекста.

Интернет-магазины, банки, платежные системы

В общем определении категория включает в себя веб-ресурсы, предназначенные для проведения любых операций с безналичными денежными средствами в онлайн-режиме с помощью специальных вебприложений. А также веб ресурсы, помогающие снять, сдать, купить или продать недвижимость.

- Интернет-магазины

Интернет-магазины и интернет-аукционы, предназначенные для реализации любых товаров, работ или услуг физическим и/или юридическим лицам, в том числе как веб-сайты магазинов, осуществляющих реализацию исключительно в интернете, так и интернет-представительства обычных магазинов, характерной особенностью которых является возможность оплаты в онлайн-режиме.

- Банки

  Веб-ресурсы банков.

- Платежные системы

  К данной категории относятся следующие веб страницы:

  - Специальные веб-страницы банков, предусматривающие услуги интернет-банка, включающие безналичные (электронные) переводы между банковскими счетами, открытие банковских вкладов, конвертацию денежных средств, оплату услуг сторонних организаций и т.д.

  - Веб-страницы электронных платёжных систем, предоставляющие доступ к персональной учётной записи пользователя.

- Криптовалюты и майнинг

  Подкатегория включает веб-сайты, предоставляющие сервисы покупки и продажи криптовалют, сервисы информирования о криптовалютах и майнинге.

Компьютерные игры

Данная категория включает веб-ресурсы, посвящённые компьютерным играм разнообразных жанров. А также игровые сообщества и сервисы.

Религии, религиозные объединения

Данная категория включает веб-ресурсы, содержащие материалы об общественных течениях (движениях), объединениях (сообществах) и организациях, подразумевающих наличие религиозной идеологии и/или культа в любых проявлениях.

Новостные ресурсы

Новостные порталы на любые темы, в том числе социальные новости агрегаторы новостей, rss рассылки.

Баннеры

Категория включает веб-ресурсы, содержащие баннеры. Рекламная информация на баннерах может отвлекать пользователей от дел, а загрузка баннеров увеличивает объем трафика.

Региональные ограничения законодательства

- Запрещено законодательством Российской Федерации
- Запрещено законодательством Бельгии
- Запрещено полицией Японии

  Веб-ресурсы, предоставляемые по соглашению с японской полицией, только для продуктов японского рынка.

Приложение 4. Расширения файлов для быстрой проверки съемных дисков

com – исполняемый файл программы размером не более 64 КБ; exe – исполняемый файл,

самораспаковывающийся архив; sys – системный файл Microsoft Windows; prg – текст

программы dBase™, Clipper или Microsoft Visual FoxPro®, программа пакета WAVmaker; bin –

бинарный файл; bat – файл пакетного задания; cmd – командный файл Microsoft Windows NT

(аналогичен bat-файлу для DOS), OS/2; dpl – упакованная библиотека Borland Delphi; dll –

библиотека динамической загрузки; scr – файл-заставка экрана Microsoft Windows; cpl –

модуль панели управления (control panel) в Microsoft Windows; ocx – объект Microsoft OLE

(Object Linking and Embedding); tsp – программа, работающая в режиме разделения времени;

drv – драйвер некоторого устройства; vxd – драйвер виртуального устройства Microsoft

Windows; pif – файл с информацией о программе; lnk – файл-ссылка в Microsoft Windows; reg –

файл регистрации ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых программ;

cla – класс Java;

vbs – скрипт Visual Basic®; vbe – видеорасширение BIOS; js, jse – исходный

текст JavaScript; htm – гипертекстовый документ; htt – гипертекстовая

заготовка Microsoft Windows; hta – гипертекстовая программа для

Microsoft Internet Explorer®; asp – скрипт Active Server Pages; chm –

скомпилированный HTML-файл; pht – HTML-файл со встроенными

скриптами PHP; php – скрипт, встраиваемый в HTML-файлы; wsh – файл

Microsoft Windows Script Host; wsf – скрипт Microsoft Windows; the –

файл заставки для рабочего стола Microsoft Windows 95; hlp – файл

справки формата Win Help; eml – сообщение электронной почты Microsoft

Outlook Express; nws – новое сообщение электронной почты Microsoft

Outlook Express; msg – сообщение электронной почты Microsoft Mail; plg –

сообщение электронной почты; mbx – сохраненное сообщение

электронной почты Microsoft O ice Outlook;

doc* – документы Microsoft O ice Word, такие как: doc – документ Microsoft O ice Word, docx – документ Microsoft O ice Word 2007 с поддержкой языка XML, docm – документ Microsoft O ice Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Oice Word, такие как: dot – шаблон документа Microsoft O ice Word, dotx – шаблон документа Microsoft O ice Word 2007, dotm – шаблон документа Microsoft O ice

Word 2007 с поддержкой макросов; fpm – программа баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format; shs – фрагмент Windows Shell Scrap Object Handler; dwg – база

данных чертежей AutoCAD®;

msi – пакет Microsoft Windows Installer; otm – VBA-проект для

Microsoft O ice Outlook; pdf – документ Adobe Acrobat; swf –

объект пакета Shockwave® Flash; jpg, jpeg – файл графического

формата хранения сжатых изображений; emf – файл формата

Enhanced Meta le; ico – файл значка объекта; ov? – исполняемые

файлы Microsoft O ice Word;

xl* – документы и файлы Microsoft O ice Excel, такие как: xla – расширение Microsoft O ice Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft O ice Excel 2007, xltm – рабочая книга Microsoft O ice Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft O ice Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft O ice Excel 2007, xlsm – шаблон Microsoft O ice Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft O ice Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft O ice PowerPoint®, такие как: pps – слайд Microsoft O ice PowerPoint, ppt – презентация, pptx – презентация Microsoft O ice PowerPoint 2007, pptm – презентация Microsoft O ice PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации

Microsoft O ice PowerPoint 2007, potm – шаблон презентации Microsoft O ice PowerPoint 2007 с поддержкой макросов, ppsx – слайдшоу Microsoft O ice PowerPoint 2007, ppsm – слайд-шоу Microsoft O ice PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft O ice PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Oice Access®, такие как: mda – рабочая группа Microsoft O ice Access, mdb – база данных; sldx – слайд Microsoft O ice PowerPoint

2007; sldm – слайд Microsoft O ice PowerPoint 2007 с

поддержкой макросов;

thmx – тема Microsoft O ice 2007.

Приложение 5. Типы файлов для фильтра вложений Защиты от почтовых угроз

Следует помнить, что фактический формат файла может не совпадать с форматом, указанным в расширении файла.

Если вы включили фильтрацию вложений в сообщениях электронной почты, то в результате фильтрации компонент Защита от почтовых угроз может переименовывать или удалять файлы следующих расширений:

com – исполняемый файл программы размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows; prg – текст программы dBase™, Clipper или

Microsoft Visual FoxPro®, программа пакета WAVmaker; bin – бинарный файл; bat – файл

пакетного задания; cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для

DOS), OS/2; dpl – упакованная библиотека Borland Delphi; dll – библиотека динамической

загрузки; scr – файл-заставка экрана Microsoft Windows; cpl – модуль панели управления

(control panel) в Microsoft Windows; ocx – объект Microsoft OLE (Object Linking and

Embedding); tsp – программа, работающая в режиме разделения времени; drv – драйвер

некоторого устройства; vxd – драйвер виртуального устройства Microsoft Windows; pif – файл

с информацией о программе; lnk – файл-ссылка в Microsoft Windows; reg – файл регистрации

ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых программ; cla – класс Java; vbs – скрипт Visual

Basic®; vbe – видеорасширение BIOS; js, jse – исходный текст

JavaScript; htm – гипертекстовый документ; htt –

гипертекстовая заготовка Microsoft Windows; hta –

гипертекстовая программа для Microsoft Internet Explorer®;

asp – скрипт Active Server Pages; chm – скомпилированный

HTML-файл; pht – HTML-файл со встроенными скриптами

PHP;

php – скрипт, встраиваемый в HTML-файлы; wsh – файл Microsoft

Windows Script Host; wsf – скрипт Microsoft Windows; the – файл

заставки для рабочего стола Microsoft Windows 95; hlp – файл справки

формата Win Help; eml – сообщение электронной почты Microsoft Outlook

Express; nws – новое сообщение электронной почты Microsoft Outlook

Express; msg – сообщение электронной почты Microsoft Mail; plg –

сообщение электронной почты; mbx – сохраненное сообщение

электронной почты Microsoft O ice Outlook;

doc* – документы Microsoft O ice Word, такие как: doc – документ Microsoft O ice Word, docx – документ Microsoft O ice Word 2007 с поддержкой языка XML, docm – документ Microsoft O ice Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Oice Word, такие как: dot – шаблон документа Microsoft O ice Word, dotx – шаблон документа Microsoft O ice Word 2007, dotm – шаблон документа Microsoft O ice

Word 2007 с поддержкой макросов; fpm – программа баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format; shs – фрагмент Windows Shell Scrap Object Handler; dwg – база

данных чертежей AutoCAD®; msi – пакет Microsoft Windows Installer; otm – VBA-проект для Microsoft O

ice Outlook; pdf – документ Adobe Acrobat; swf – объект пакета Shockwave® Flash; jpg, jpeg – файл

графического формата хранения сжатых изображений; emf – файл формата Enhanced Meta le; ico – файл

значка объекта; ov? – исполняемые файлы Microsoft O ice Word;

xl* – документы и файлы Microsoft O ice Excel, такие как: xla – расширение Microsoft O ice Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft O ice Excel 2007, xltm – рабочая книга Microsoft O ice Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft O ice Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft O ice Excel 2007, xlsm – шаблон Microsoft O ice Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft O ice Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft O ice PowerPoint®, такие как: pps – слайд Microsoft O ice PowerPoint, ppt – презентация, pptx – презентация Microsoft O ice PowerPoint 2007, pptm – презентация Microsoft O ice PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft O ice PowerPoint 2007, potm – шаблон презентации Microsoft O ice PowerPoint 2007 с поддержкой макросов, ppsx – слайдшоу Microsoft O ice PowerPoint 2007, ppsm – слайд-шоу Microsoft O ice PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft O ice PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Oice Access®, такие как: mda – рабочая группа Microsoft O ice Access, mdb – база данных; sldx – слайд Microsoft O ice PowerPoint

2007; sldm – слайд Microsoft O ice PowerPoint 2007 с

поддержкой макросов; thmx – тема Microsoft O ice 2007.

Информация о стороннем коде

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Acrobat, Flash, Reader и Shockwave – товарные знаки или зарегистрированные в Соединенных Штатах Америки и / или в других странах товарные знаки Adobe Systems Incorporated.

Apple, FireWire, iTunes и Safari – товарные знаки Apple Inc., зарегистрированные в США и других странах.

AutoCAD – товарный знак или зарегистрированный в США и/или других странах товарный знак, принадлежащий Autodesk, Inc. и / или дочерним / аффилированным компаниям.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Borland – товарный знак или зарегистрированный товарный знак Borland Software Corporation.

Android, Chrome, Google Chrome и Google Talk – товарные знаки Google, Inc.

Citrix, Citrix Provisioning Services, XenApp и XenDesktop – товарные знаки Citrix Systems, Inc. и/или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

dBase – товарный знак dataBased Intelligence, Inc.

EMC и SecurID – зарегистрированные товарные знаки или товарные знаки EMC Corporation в США и/или других странах.

Radmin – зарегистрированный товарный знак Famatech.

IBM – товарный знак International Business Machines Corporation, зарегистрированный во многих юрисдикциях по всему миру.

ICQ – товарный знак и/или знак обслуживания ICQ LLC.

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

IOS – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и / или ее аффилированных компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Logitech является зарегистрированным товарным знаком или товарным знаком компании Logitech в США и (или) других странах.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Segoe, Skype, Visual C++, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server и Windows Store – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla, Firefox и Thunderbird – товарные знаки Mozilla Foundation.

Java и JavaScript – зарегистрированные товарные знаки компании Oracle и/или ее аффилированных компаний.

VMware и VMware ESXi – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.