

kaspersky

Kaspersky Endpoint Detection and Response Optimum

Руководство по эксплуатации

Версия программы: 2.0

Содержание

[Справка Kaspersky Endpoint Detection and Response Optimum 2.0](#)

[О Kaspersky Endpoint Detection and Response Optimum](#)

[Что нового](#)

[Программные требования](#)

[Архитектура решения](#)

[Известные ограничения](#)

[Лицензирование](#)

[О Лицензионном соглашении](#)

[О лицензии](#)

[О лицензионном сертификате](#)

[О лицензионном ключе](#)

[О коде активации](#)

[О файле ключа](#)

[О Kaspersky Security Network](#)

[О предоставлении данных](#)

[Активация Kaspersky Endpoint Detection and Response Optimum](#)

[Поддерживаемые конфигурации и сценарии развертывания](#)

[Развертывание и первоначальная настройка Kaspersky Endpoint Detection and Response Optimum 2.0](#)

[Обновление предыдущей версии Kaspersky Endpoint Detection and Response Optimum](#)

[Сценарий: локальное обновление через Kaspersky Security Center Web Console](#)

[Сценарий: облачное обновление через Kaspersky Security Center Cloud Console](#)

[Совместная работа с другими решениями "Лаборатории Касперского"](#)

[Действия по реагированию на обнаружения](#)

[Сетевая изоляция](#)

[Помещение файла на карантин](#)

[Удаление файла](#)

[Запуск проверки важных областей](#)

[Поиск IOC](#)

[Запрет запуска объектов](#)

[Запуск процесса](#)

[Завершение процесса](#)

[Получение файла](#)

[Работа с деталями обнаружения](#)

[О деталях обнаружения](#)

[Настройка отчета об угрозах для отображения деталей обнаружений](#)

[Просмотр деталей обнаружения](#)

[Сетевая изоляция устройства из деталей обнаружения](#)

[Помещение файла на карантин из деталей обнаружения](#)

[Создание задачи поиска IOC из деталей обнаружения](#)

[Запрет запуска файла из деталей обнаружения](#)

[Мониторинг и отчеты](#)

[Добавление виджета EDR-обнаружений](#)

[Просмотр списка обнаружений](#)

[Проверка работоспособности Kaspersky Endpoint Detection and Response Optimum на устройствах](#)

[Просмотр информации о срабатывании правил запрета запуска](#)

[Получение списка изолированных устройств](#)

[Мультиотенантность](#)

[Источники информации о программе](#)

[Обращение в Службу технической поддержки](#)

[Способы получения технической поддержки](#)

[Техническая поддержка по телефону](#)

[Техническая поддержка через Kaspersky CompanyAccount](#)

[Глоссарий](#)

[Endpoint Protection Platform \(EPP\)](#)

[EPP-программа](#)

[IOC](#)

[IOC-файл](#)

[OpenIOC](#)

[TLS-шифрование](#)

[Действие по реагированию](#)

[Тенант](#)

[Трассировка](#)

[Целевая атака](#)

[Информация о стороннем коде](#)

[Уведомления о товарных знаках](#)

Справка Kaspersky Endpoint Detection and Response Optimum
2.0



[Что нового](#)



[Аппаратные и программные требования](#)



[Лицензирование](#)



[Развертывание и первоначальная настройка решения](#)



[Обновление предыдущей версии](#)



[Обращение в Службу технической поддержки](#)



Ключевые функции

- [Сетевая изоляция устройства](#)
- [Запрет запуска объектов](#)
- [Поиск ИОС](#)
- [Просмотр списка обнаружений в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console](#)
- [Виджет EDR обнаружений в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console](#)

О Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum (далее также EDR Optimum) – решение, предназначенное для защиты IT-инфраструктуры организации от сложных кибернетических угроз. Функционал решения сочетает автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противостояния сложным атакам, в том числе новым эксплойтам (англ. exploits), программам-шантажистам (англ. ransomware), бесфайловым атакам (англ. fileless attacks), а также методам, использующим законные системные инструменты.

Kaspersky Endpoint Detection and Response Optimum выполняет обзор и анализ развития угрозы и предоставляет сотруднику службы безопасности или администратору [информацию о потенциальной атаке](#), необходимую для принятия своевременных [действий по реагированию](#), или применяет заданные действия по реагированию автоматически.

Что нового

В версии Kaspersky Endpoint Detection and Response Optimum 2.0 добавлены следующие новые функции и улучшения:

- Встроенная функциональность [EDR Optimum в Kaspersky Endpoint Security для Windows](#)  позволяет использовать решение без установки дополнительного программного обеспечения.
- Функциональность [мультиотенантности](#) позволяет предоставлять услуги Kaspersky Endpoint Detection and Response Optimum в качестве поставщика для других организаций.
- Появилась возможность [снять сетевую изоляцию устройства из деталей обнаружения](#).
- Срок хранения подробных результатов выполнения задачи поиска ИОС увеличен до одного месяца.
- Снято ограничение на количество процессов, которые могут отображаться в [деталях обнаружения](#).
- Появилась возможность [просматривать результаты выполнения задачи запуска процесса](#) .
- [Получение файла](#) стало доступным в качестве отдельной задачи.
- [Обновление EDR Optimum](#)  [с предыдущей версии](#) оптимизировано с помощью мастера миграции политик и задач.
- Размер [деталей обнаружения](#), которые хранятся на сервере и доступны для просмотра независимо от подключения к устройству, увеличен до 1 МБ.
- Изменена терминология решения. Термин "incident" был заменен на "alert" в английской локализации, что повлекло изменения во всех остальных языках. В русской локализации произошла замена термина "оповещение" на "обнаружение".
- Добавлена поддержка новых локализаций для пользовательского интерфейса и онлайн-справки.

Программные требования

Kaspersky Endpoint Detection and Response Optimum 2.0 поддерживается следующими версиями программ "Лаборатории Касперского":

- EPP-программы:
 - Kaspersky Endpoint Security для Windows – версия 11.7 и выше.
- Программы для централизованного управления безопасностью сети:

- Kaspersky Security Center Web Console – версия 13.2 и выше;
- Kaspersky Security Center Cloud Console.

Информацию об аппаратных и программных требованиях поддерживаемых программ см. в справке программ "Лаборатории Касперского", установленных в вашей IT-инфраструктуре:

- [Kaspersky Endpoint Security для Windows](#) 
- [Kaspersky Security Center Web Console](#) 
- [Kaspersky Security Center Cloud Console](#) 

Архитектура решения

В состав решения Kaspersky Endpoint Detection and Response Optimum 2.0 входят следующие компоненты:

- [EPP-программы с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum](#), которые устанавливаются на отдельные устройства, входящие в IT-инфраструктуру организации. Эти программы осуществляют постоянное наблюдение за процессами, запущенными на защищаемых устройствах, открытыми сетевыми соединениями и изменяемыми файлами.
- Решение для централизованного управления сетевой безопасностью (Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console).
- Kaspersky Sandbox (опциональный компонент, приобретается отдельно), предназначенный для дополнительной проверки подозрительных объектов, обнаруженных EPP-программой. Подробную информацию о Kaspersky Sandbox см. в *Справке Kaspersky Sandbox*.
- Средства анализа угроз (Threat Intelligence):
 - Инфраструктура облачных служб [Kaspersky Security Network](#) (далее также KSN), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.
 - Интеграция с решением [Kaspersky Private Security Network](#) , предоставляющим возможность получать доступ к репутационным базам KSN, а также другим статистическим данным, не отправляя в KSN данные со своих компьютеров.
 - Интеграция с платформой [Kaspersky Threat Intelligence Portal](#) , которая содержит и отображает информацию о репутации файлов и веб-адресов.

- База угроз [Kaspersky Threats](#) .

Известные ограничения

Kaspersky Endpoint Detection and Response Optimum версии 2.0 имеет следующие ограничения:

- Решение поддерживается только начиная с версии KESWin 11.7 и выше. Для остальных EPP-программ необходимо продолжать использовать EDR Optimum [более ранней версии](#).
- [Совместная работа с Kaspersky Sandbox 1.0](#) не поддерживается.
- Детали обнаружения и подробные результаты выполнения задачи поиска IOC удаляются по истечении одного месяца после создания.
- Функциональность мультитенантности имеет ряд ограничений. Подробнее см. в разделе [Мультитенантность](#).

Лицензирование

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

Подробнее о лицензировании программ, входящих в состав решения Kaspersky Endpoint Detection and Response Optimum 2.0 см. в справке программы:

- [Kaspersky Endpoint Security для Windows](#) .
- [Kaspersky Security Center Web Console](#) .
- [Kaspersky Security Center Cloud Console](#) .

О Лицензионном соглашении

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

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Endpoint Detection and Response Optimum.

- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

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 и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании 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 имеет небольшой срок действия. По истечении срока действия пробной лицензии EDR Optimum 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.

По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Endpoint Detection and Response Optimum). Чтобы продолжить использование Kaspersky Endpoint Detection and Response Optimum 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 лицензионном ключе

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

Вы можете добавить лицензионный ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы программы требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (или резервным).

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

Дополнительный (или резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

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 Detection and Response Optimum. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Detection and Response Optimum или после заказа пробной версии Kaspersky Endpoint Detection and Response Optimum.

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

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 Detection and Response Optimum или после заказа пробной версии Kaspersky Endpoint Detection and Response Optimum.

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.

О Kaspersky Security Network

Kaspersky Security Network (далее также *KSN*) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования *KSN*, вы можете прочитать на [веб-сайте "Лаборатории Касперского"](#) .

Инфраструктура *KSN*

В *Kaspersky Security Network* есть следующие инфраструктурные решения:

- *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 Detection and Response Optimum* 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.

О предоставлении данных

Для корректной работы компонентов *Kaspersky Endpoint Detection and Response Optimum* требуется обработка данных на стороне "Лаборатории Касперского".

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Подробную информацию о данных, предоставляемых при использовании решения *Kaspersky Endpoint Detection and Response Optimum 2.0*, см. в справке программ "Лаборатории Касперского", установленных в вашей ИТ-инфраструктуре:

- [Kaspersky Endpoint Security для Windows](#) ;
- [Kaspersky Security Center Web Console](#) ;
- [Kaspersky Security Center Cloud Console](#) .

Активация Kaspersky Endpoint Detection and Response Optimum

Активация решения Kaspersky Endpoint Detection and Response Optimum 2.0 заключается в активации EPP-программ, установленных на защищаемых устройствах, с помощью лицензии, которая включает функциональность Kaspersky Endpoint Detection and Response Optimum 2.0.

Вы можете приобрести лицензию на использование функциональности Kaspersky Endpoint Detection and Response Optimum 2.0 следующими способами:

- в составе лицензии на использование EPP-программы;
- отдельно, в дополнение к ранее приобретенной лицензии на использование EPP-программы.

Если ваша лицензия на использование программы на устройствах включает функциональность Kaspersky Endpoint Detection and Response Optimum 2.0, то эта функциональность станет доступна после выполнения [первоначальной настройки решения](#).

Если вы приобрели лицензию на использование Kaspersky Endpoint Detection and Response Optimum 2.0 отдельно, в дополнение к ранее приобретенной лицензии уже после установки и активации программ "Лаборатории Касперского" на устройства, то необходимо активировать программы на устройствах повторно с помощью нового кода активации или файла ключа, в зависимости от способа, которым вы приобрели лицензию на использование Kaspersky Endpoint Detection and Response Optimum 2.0. После этого необходимо выполнить [первоначальную настройку решения](#).

Подробнее об активации решения см. в [справке Kaspersky Endpoint Security для Windows](#) .

Поддерживаемые конфигурации и сценарии развертывания

Информацию о минимальных поддерживаемых версиях программ "Лаборатории Касперского" для защиты IT-инфраструктуры см. в разделе [Программные требования](#).

Возможны следующие сценарии развертывания:

- Первичная установка и развертывание программ для защиты IT-инфраструктуры и решения Kaspersky Endpoint Detection and Response Optimum 2.0, либо установка Kaspersky Endpoint Detection and Response Optimum 2.0 в инфраструктуре, в которой ранее уже были установлены поддерживаемые версии программ для защиты IT-

инфраструктуры. Подробнее см. в разделе [Развертывание и первоначальная настройка Kaspersky Endpoint Detection and Response Optimum 2.0](#).

- Развертывание в инфраструктуре, где уже используется версия Kaspersky Endpoint Detection and Response Optimum 1.1 или более ранняя, с программами для защиты IT-инфраструктуры разных версий и предназначенными для разных типов устройств с разными операционными системами. Подробнее см. в разделе [Обновление предыдущей версии Kaspersky Endpoint Detection and Response Optimum](#).

Развертывание и первоначальная настройка Kaspersky Endpoint Detection and Response Optimum 2.0

Развертывание решения Kaspersky Endpoint Detection and Response Optimum 2.0 включает в себя следующие этапы:

1 Установка решения для централизованного управления безопасностью сети

[Установите Kaspersky Security Center Web Console](#)  или используйте [Kaspersky Security Center Cloud Console](#)  для управления решением Kaspersky Endpoint Detection and Response Optimum в вашей инфраструктуре.

2 Установка EPP-программ

Установите EPP-программы с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum 2.0 на устройства, которые требуется защищать.

Kaspersky Endpoint Detection and Response Optimum 2.0 поддерживается начиная с версии Kaspersky Endpoint Security для Windows 11.7 и Kaspersky Security Center Web Console 13.2. Подробную информацию о поддерживаемых версиях программ см. в разделе [Программные требования](#).

Информацию об установке см. в справке [Kaspersky Endpoint Security для Windows](#) .

3 Установка веб-плагина

Установите веб-плагин EPP-программы для Kaspersky Security Center Web Console.

Веб-плагины для Kaspersky Security Center Cloud Console встроены по умолчанию.

Информацию об установке веб-плагина см. в справке [Kaspersky Endpoint Security для Windows](#) .

4 Активация Kaspersky Endpoint Detection and Response Optimum

Если ваша лицензия на использование EPP-программ на устройствах включает функциональность Kaspersky Endpoint Detection and Response Optimum 2.0, дополнительных действий не требуется.

Если вы приобрели лицензию на использование Kaspersky Endpoint Detection and Response Optimum 2.0 после установки программ "Лаборатории Касперского" на устройства, [активируйте решение](#).

5 Создание политики в Kaspersky Security Center

Создайте политики, которые будут распространяться на группы устройств, защищаемых EPP-программами.

Информацию о создании политик см. в справке [Kaspersky Endpoint Security для Windows](#).

6 Включение Kaspersky Endpoint Detection and Response Optimum на устройствах

Выполните интеграцию с EPP-программами и включите решение Kaspersky Endpoint Detection and Response Optimum в параметрах EPP-программы на устройствах. Подробнее см. в справке [Kaspersky Endpoint Security для Windows](#).

7 Настройка отчета об угрозах

[Настройте отчет об угрозах](#) для просмотра деталей обнаружения.

8 Добавление виджета

Добавьте [виджет EDR-обнаружений](#).

9 Отображение списка обнаружений

Включите отображение раздела **Обнаружения** в [Kaspersky Security Center Web Console](#) или [Kaspersky Security Center Cloud Console](#).

Обновление предыдущей версии Kaspersky Endpoint Detection and Response Optimum

Развертывание в инфраструктуре, где уже используется Kaspersky Endpoint Detection and Response Optimum версии 1.1 или более ранней, с программами для защиты IT-инфраструктуры разных версий и предназначенными для разных типов устройств с разными операционными системами, различается в зависимости от того, какую программу вы используете для централизованного управления безопасностью сети:

- *Локальная* программа - это Kaspersky Security Center Web Console.
- *Облачная* программа - это Kaspersky Security Center Cloud Console.

Подробнее см. [в справке Kaspersky Security Center](#).

Сценарий: локальное обновление через Kaspersky Security Center Web Console

Локальное обновление решения Kaspersky Endpoint Detection and Response Optimum 2.0 включает в себя следующие этапы:

1 Обновление решения для централизованного управления безопасностью сети

Обновите Kaspersky Security Center до версии 13.2, включая компоненты программы Агент администрирования на компьютерах пользователей и [Kaspersky Security Center Web Console](#) .

Kaspersky Endpoint Detection and Response Optimum 2.0 поддерживается начиная с версии Kaspersky Security Center Web Console 13.2.

2 Установка новой версии веб-плагина

Установите веб-плагин EPP-программы для Kaspersky Security Center Web Console с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum 2.0.

Kaspersky Endpoint Detection and Response Optimum 2.0 поддерживается начиная с версии Kaspersky Endpoint Security для Windows 11.7.

Информацию об установке веб-плагина см. в *Справке* [Kaspersky Endpoint Security для Windows](#).

3 Выполнение шагов мастера миграции политик и задач

Запустите [мастер миграции политик и задач](#)  и выполните все шаги мастера.

4 Обновление EPP-программ

Обновите EPP-программы до версии с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum 2.0 на устройствах, которые требуется защищать.

Kaspersky Endpoint Detection and Response Optimum 2.0 поддерживается начиная с версии Kaspersky Endpoint Security для Windows 11.7. Подробную информацию о поддерживаемых версиях программ см. в разделе [Программные требования](#).

Информацию об [обновлении](#)  и [миграции конфигурации на Kaspersky Endpoint Security 11.7](#) см. в *Справке Kaspersky Endpoint Security для Windows*.

Устройства под защитой Kaspersky Endpoint Detection and Response Optimum 1.1 и более ранней версии, на которых отсутствует возможность обновить EPP-программу до версии с поддержкой Kaspersky Endpoint Detection and Response Optimum 2.0, остаются под защитой предыдущей версии Kaspersky Endpoint Detection and Response Optimum. Подробнее см. в разделе [Совместная работа с другими решениями "Лаборатории Касперского"](#).

Сценарий: облачное обновление через Kaspersky Security Center Cloud Console

Облачное обновление решения Kaspersky Endpoint Detection and Response Optimum 2.0 включает в себя следующие этапы:

1 Обновление Агента администрирования

Обновите Агент администрирования Kaspersky Security Center до версии с поддержкой Kaspersky Endpoint Detection and Response Optimum.

2 Выполнение шагов мастера миграции политик и задач

Запустите [мастер миграции политик и задач](#) и выполните все шаги мастера.

3 Обновление EPP-программ

Обновите EPP-программы до версии с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum 2.0 на устройствах, которые требуется защищать.

Kaspersky Endpoint Detection and Response Optimum 2.0 поддерживается начиная с версии Kaspersky Endpoint Security для Windows 11.7. Подробную информацию о поддерживаемых версиях программ см. в разделе [Программные требования](#).

Информацию об [обновлении](#) и [миграции конфигурации на Kaspersky Endpoint Security 11.7](#) см. в *Справке Kaspersky Endpoint Security для Windows*.

Устройства под защитой Kaspersky Endpoint Detection and Response Optimum версии 1.1 и более ранней, на которых отсутствует возможность обновить EPP-программу до версии с поддержкой Kaspersky Endpoint Detection and Response Optimum 2.0, остаются под защитой предыдущей версии Kaspersky Endpoint Detection and Response Optimum. Подробнее см. в разделе [Совместная работа с другими решениями "Лаборатории Касперского"](#).

Совместная работа с другими решениями "Лаборатории Касперского"

Совместная работа с предыдущими версиями EDR Optimum

При обновлении Kaspersky Endpoint Detection and Response Optimum 2.0 только на выборочных устройствах в вашей инфраструктуре часть устройств останется под защитой более ранних версий Kaspersky Endpoint Detection and Response Optimum. Работу более ранних версий EDR Optimum будет по-прежнему обеспечивать веб-плагин программы Kaspersky Endpoint Agent. Подробнее см. в разделе [Обновление предыдущей версии Kaspersky Endpoint Detection and Response Optimum](#).

Совместная работа с Kaspersky Sandbox

Если в вашей инфраструктуре также используется решение Kaspersky Sandbox, то работу этого решения на устройствах по-прежнему обеспечивает веб-плагин программы Kaspersky Endpoint Agent.

Решение Kaspersky Endpoint Detection and Response Optimum 2.0 совместимо с Kaspersky Sandbox начиная с версии 2.0. При этом для синхронных обнаружений Kaspersky Sandbox вы сможете открыть [детали обнаружения](#), предоставляемые функциональностью Kaspersky Endpoint Detection and Response Optimum.

При совместной работе разных версий Kaspersky Endpoint Detection and Response Optimum и Kaspersky Sandbox внутри одной инфраструктуры необходимо обеспечить отдельный сервер Kaspersky Sandbox для версии 1.0 для тех устройств, которые остаются под защитой Kaspersky Endpoint Detection and Response Optimum 1.1 и более ранних версий, и отдельный сервер Kaspersky Sandbox 2.0 для тех устройств, которые работают под защитой Kaspersky Endpoint Detection and Response Optimum 2.0.

Совместная работа с Kaspersky MDR

Лицензия на использование решения Kaspersky Managed Detection and Response позволяет также использовать и решение EDR Optimum. При этом для реагирования на инциденты Kaspersky MDR будет доступна часть действий по реагированию, обеспечиваемых решением EDR Optimum. Если оба решения одновременно применяют одно и то же действие по реагированию, то оно применяется только в рамках работы одного из решений.

Действия по реагированию, которые были предложены аналитиками SOC и приняты офицером безопасности в рамках работы Kaspersky MDR, не будут отображаться в параметрах, политиках и задачах EDR Optimum.

Действия по реагированию на обнаружения

Этот раздел содержит информацию о действиях по реагированию на обнаруженные угрозы, доступных в рамках функциональности Kaspersky Endpoint Detection and Response Optimum 2.0.

Сетевая изоляция

Kaspersky Endpoint Detection and Response Optimum предоставляет возможность изолировать устройства от сети по требованию (вручную) или в качестве автоматического действия по реагированию на обнаруженные угрозы.

После включения сетевой изоляции программа разрывает все активные и блокирует все новые сетевые соединения TCP/IP на устройствах, кроме следующих соединений:

- соединения, указанные в исключениях из сетевой изоляции;
- соединения, инициированные службами совместимой EPP-программы;
- соединения, инициированные Агентом администрирования Kaspersky Security Center.

Сетевая изоляция устройства может быть применена вручную в параметрах EPP-программы на устройстве или [в деталях обнаружения](#), а также автоматически, в результате ответных действий на обнаружения при выполнении задачи поиска ИОС. Разблокировать изолированное устройство можно вручную из деталей обнаружения, в параметрах EPP-программы на устройстве или из командной строки, а также можно настроить период, по истечении которого требуется выключать сетевую изоляцию автоматически.

Вы можете настроить исключения из сетевой изоляции. Сетевые соединения, подпадающие под заданные исключения, не будут заблокированы на устройствах после включения сетевой изоляции.

Подробнее об управлении сетевой изоляцией вручную через параметры EPP-программы на устройстве, настройке параметров автоматического применения сетевой изоляции через политику Kaspersky Security Center, настройке исключений и возможностях управления сетевой изоляцией через командную строку см. в справке [Kaspersky Endpoint Security для Windows](#) .

Помещение файла на карантин

Одним из возможных действий по реагированию при обнаружении угрозы является помещение файла на карантин.

Карантин – это специальное локальное хранилище на устройстве с [EPP-программой, поддерживающей функциональность Kaspersky Endpoint Detection and Response Optimum](#), в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения. Файлы на карантине хранятся на защищаемом устройстве в зашифрованном виде и не угрожают безопасности устройства.

Файл может быть помещен на карантин вручную или автоматически, в результате [ответных действий на обнаружения](#).

Подробнее о создании задачи помещения файла на карантин см. в справке [Kaspersky Endpoint Security для Windows](#) . Вы также можете [поместить файл на карантин из деталей обнаружения](#) .

Чтобы просмотреть список файлов в карантине,

в главном окне Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Хранилища** → **Карантин**.

Подробнее о работе с карантинном см. в справке [Kaspersky Security Center](#) .

Проверка объектов, помещенных на карантин в рамках работы Kaspersky Endpoint Detection and Response Optimum, недоступна.

Восстановление файлов из карантина также доступно из командной строки. Подробнее см. в справке [Kaspersky Endpoint Security для Windows](#) .

Объекты помещаются на карантин под системной учетной записью (SYSTEM). При восстановлении из карантина файл помещается не в исходное расположение, а в специальную папку на устройстве, из которой вы сможете вручную переместить его в папку назначения.

Чтобы настроить параметры хранения файлов в карантине, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики, которую вы хотите настроить.
Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. В разделе **Репозитории** выберите подраздел **Карантин** и задайте нужные параметры.
Информацию о доступных для настройки параметрах карантина см. в справке [Kaspersky Endpoint Security для Windows](#) .

Удаление файла

Одним из возможных действий по реагированию при обнаружении угрозы является удаление файла с устройства.

Подробнее о создании задачи удаления файла см. в справке [Kaspersky Endpoint Security для Windows](#).

Запуск проверки важных областей

Одним из возможных действий по реагированию при обнаружении угрозы является запуск на устройстве проверки важных областей.

Проверка важных областей может быть запущена вручную или автоматически, в результате [ответных действий на обнаружения](#).

Подробнее о проверке важных областей см. в справке [Kaspersky Endpoint Security для Windows](#).

Поиск IOC

Индикатор компрометации (англ. Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к устройству (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему. Задача поиска IOC позволяет обнаруживать индикаторы компрометации на устройстве и выполнять действия по реагированию на угрозы.

Для поиска IOC используются [IOC-файлы](#) (файлы, содержащие набор индикаторов, при совпадении с которыми EPP-программа считает событие обнаружением). IOC-файлы должны соответствовать стандарту описания OpenIOC.

В Kaspersky Endpoint Detection and Response Optimum предусмотрены следующие режимы запуска задач поиска IOC:

- *Стандартная задача поиска IOC* – групповая или локальная задача, которая создается и настраивается вручную в Kaspersky Security Center Web Console. Для запуска задач используются IOC-файлы, подготовленные пользователем.
- *Автономная задача поиска IOC* – групповая задача, которая создается автоматически при реагировании на угрозу, обнаруженную [Kaspersky Sandbox](#). EPP-программа автоматически формирует IOC-файл. Работа с пользовательскими IOC-файлами не предусмотрена. Задачи автоматически удаляются через семь дней после последнего запуска или с момента создания, если задачи не запускались. Подробнее об автономных задачах поиска IOC см. в справке [Kaspersky Sandbox](#).

При обнаружении IOC на устройстве Kaspersky Endpoint Detection and Response Optimum выполняет заданное действие по реагированию. Доступны следующие действия по реагированию на обнаруженные IOC:

- [Изолировать устройство от сети](#).

- [Запускать проверку важных областей.](#)

- [Копию поместить на карантин, объект удалить.](#)

При реагировании на угрозы Kaspersky Endpoint Detection and Response Optimum и Kaspersky Sandbox могут автоматически создавать задачи поиска ИОС. Вы также можете создать задачу вручную [из деталей обнаружения](#) или в [Kaspersky Endpoint Security для Windows](#) .

Запуск задач поиска ИОС доступен [из командной строки](#) .

Запрет запуска объектов

Вы можете настраивать правила запрета запуска исполняемых файлов и скриптов, а также открытия файлов офисного формата на выбранных устройствах. Например, вы можете запретить запуск программ, использование которых считается небезопасным, на выбранном устройстве, защищаемом Kaspersky Endpoint Detection and Response Optimum. Программа идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Правило запрета запуска – это набор критериев, которые учитываются при выполнении блокировки. Объект должен соответствовать всем критериям правила защиты, чтобы программа заблокировала его исполнение.

Kaspersky Endpoint Detection and Response Optimum предусматривает следующие режимы применения правил запрета запуска:

- Блокирование и запись в отчет. В этом режиме EPP-программа блокирует исполнение объектов или открытие документов, соответствующих критериям правил запрета.
- Только запись события в отчет. В этом режиме EPP-программа публикует в Журнал событий Windows и Kaspersky Security Center событие о попытках исполнения объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их исполнение или открытие.

Информацию о включении, о доступных для настройки параметрах запрета запуска и об управлении правилами запрета запуска из командной строки см. в справке [Kaspersky Endpoint Security для Windows](#) .

Вы также можете запретить запуск файла [из деталей обнаружения](#).

Запуск процесса

Задача запуска процесса позволяет удаленно запускать файлы на устройстве. Например, вы можете удаленно запустить утилиту, которая создает файл с конфигурацией компьютера, и затем получить созданный файл с помощью задачи [получения файла](#).

Подробнее о создании задачи запуска процесса см. в справке [Kaspersky Endpoint Security для Windows](#).

Завершение процесса

Задача завершения процесса позволяет удаленно завершать процессы на устройстве. Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи [запуска процесса](#).

Подробнее о создании задачи завершения процесса см. в справке [Kaspersky Endpoint Security для Windows](#).

Получение файла

Задача получения файла позволяет получать файлы с устройств пользователей. Например, вы можете настроить получение файла журнала событий, который создает сторонняя программа. В результате выполнения задачи файл будет сохранен в карантине. Вы можете загрузить этот файл на компьютер из карантина в Kaspersky Security Center Web Console. При этом на компьютере пользователя файл остается в исходной папке.

Подробнее о создании задачи получения файла см. в справке [Kaspersky Endpoint Security для Windows](#).

Работа с деталями обнаружения

Этот раздел содержит информацию о действиях, которые можно выполнять непосредственно из деталей обнаружения.

О деталях обнаружения

Детали обнаружения содержат всю доступную информацию об обнаруженной угрозе и позволяют управлять [действиями по реагированию на обнаружение](#).

В деталях обнаружения может быть приведена следующая информация:

- Граф цепочки развития угрозы, который предоставляет визуальную информацию о задействованных объектах, например, о ключевых процессах на устройстве, сетевых соединениях, библиотеках, кустах реестра. Он предназначен для анализа причин появления угрозы.
- Общая информация об обнаружении, включая режим обнаружения (например, обнаружение при проверке по требованию или при автоматической проверке).
- Информация о защищаемом устройстве, на котором произошло обнаружение (например, имя, IP-адрес, MAC-адрес, список пользователей, операционная система).

- Информация об обнаруженном объекте.
- Изменения в реестре, связанные с обнаружением.
- История появления файлов на устройстве.
- Принятые программой ответные действия.

Из деталей обнаружения вы можете выполнить следующие действия по реагированию:

- [изолировать устройство, на котором произошло обнаружение](#);
- [поместить файл на карантин](#);
- [создать задачу поиска ИОС](#);
- [запретить запуск обнаруженного файла](#).

Детали обнаружения автоматически удаляются через один месяц после того, как были сформированы.

Если объем информации в деталях обнаружения превышает 1 МБ или если за сутки на устройстве появилось больше пяти обнаружений, то данные об обнаружении хранятся на этом устройстве локально и для доступа к ним необходимо подключение к этому устройству.

Настройка отчета об угрозах для отображения деталей обнаружений

Чтобы настроить возможность перейти в детали обнаружения из отчета об угрозах, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. В списке отчетов установите флажок для отчета шаблона **Отчет об угрозах** и нажмите на кнопку **Открыть свойства шаблона отчета**.
3. В открывшемся окне изменения отчета перейдите на закладку **Графы**.

4. Убедитесь, что в блоке параметров **Детальные данные** в списке полей отчета присутствует поле с именем **Открыть обнаружение**.
5. Если поле **Открыть обнаружение** отсутствует в списке, выполните следующие действия:
 - a. Нажмите на кнопку **Добавить**.
 - b. В правой части окна в раскрывающемся списке выберите поле с именем **Открыть обнаружение**.
 - c. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**.

Просмотр деталей обнаружения настроен в параметрах отчета об угрозах.

Просмотр деталей обнаружения

Детали обнаружения доступны в окне со списком обнаружений. Список обнаружений доступен в отчете **Отчет об угрозах** или в подразделе **Обнаружения** в разделе **Мониторинг и отчеты** в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

Если вы добавите лицензионный ключ для Kaspersky Endpoint Detection and Response Optimum, подраздел **Обнаружения** автоматически отобразится в главном меню в разделе **Мониторинг и отчеты**. Вы также можете настроить отображение подраздела **Обнаружения** в свойствах интерфейса в [Kaspersky Security Center Web Console](#)  или [Kaspersky Security Center Cloud Console](#) .

Чтобы просмотреть детали обнаружения:

1. В главном окне Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Мониторинг и отчеты** → **Обнаружения**.
2. Выберите обнаружение и нажмите на ссылку **Подробнее**.
Отобразятся детали обнаружения.

Чтобы просмотреть детали обнаружения в отчете об угрозах:

1. В главном окне Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Выберите отчет шаблона **Отчет об угрозах** и нажмите на кнопку **Показать отчет**.

3. В окне отчета на вкладке **Подробнее** выберите обнаружение и нажмите на ссылку **Открыть детали обнаружения**.

Отобразятся детали обнаружения.

Сетевая изоляция устройства из деталей обнаружения

Чтобы изолировать устройство от сети или снять сетевую изоляцию устройства из деталей обнаружения, выполните следующие действия:

1. [Откройте детали обнаружения](#).

2. В блоке **Компьютер** нажмите на кнопку:

- **Изолировать компьютер от сети** – чтобы применить сетевую изоляцию к этому устройству.
- **Разблокировать изолированный от сети компьютер** – чтобы снять сетевую изоляцию с этого устройства.

Помещение файла на карантин из деталей обнаружения

Чтобы поместить файл на карантин из деталей обнаружения, выполните следующие действия:

1. [Откройте детали обнаружения](#).

2. В блоке **Файл** нажмите на кнопку **Поместить на карантин**.

Файл будет удален с устройства, а его копия будет [помещена на карантин](#).

Создание задачи поиска ИОС из деталей обнаружения

Чтобы создать задачу [поиска ИОС](#) из деталей обнаружения, выполните следующие действия:

1. [Откройте детали обнаружения](#).

2. На закладке **Все события обнаружения** выберите элементы списка, на основе которых вы хотите создать задачу поиска ИОС.

3. Нажмите на кнопку **Создать ИОС**.

4. Выберите условие срабатывания индикатора компрометации:

- Если вы хотите, чтобы ИОС срабатывал при обнаружении любого из выбранных объектов, в правой части экрана выберите **ИЛИ**.

- Если вы хотите, чтобы IOC срабатывал только при обнаружении всех выбранных объектов, в правой части экрана выберите **И**.

5. Выберите действия, которые необходимо применять при срабатывании IOC:

- [Изолировать устройство от сети](#).
- [Запускать проверку важных областей](#).
- [Копию поместить на карантин, объект удалить](#).

6. Нажмите на кнопку **Создать задачу**.

Вы можете просмотреть созданные задачи в разделе **Устройства** → **Задачи**.

При создании задачи поиска IOC из деталей обнаружения для выбранного объекта (файла или процесса) будет автоматически создан [IOC](#) с термином **FileItem**.
Подробнее о терминах IOC см. в [справке Kaspersky Endpoint Security для Windows](#).

Запрет запуска файла из деталей обнаружения

Для выполнения правил запрета запуска на устройстве, на котором произошло обнаружение, к этому устройству должна быть применена активная политика EPP-программы с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum. Если устройство, на котором произошло обнаружение, не находится под управлением активной политики, то правило запрета запуска не будет создано.

Чтобы запретить запуск файла из деталей обнаружения, выполните следующие действия:

1. [Откройте детали обнаружения](#).

2. В блоке **Файл** нажмите на кнопку **Запретить запуск**.

Запуск файла будет [запрещен](#). Правило запрета запуска будет добавлено в политику для группы, в которую входит устройство.

Мониторинг и отчеты

Для мониторинга работы решения Kaspersky Endpoint Detection and Response Optimum доступны следующие возможности:

- виджет EDR-обнаружений;

- список обнаружений;
- отчеты и выборки Kaspersky Security Center.

Добавление виджета EDR-обнаружений

В виджете EDR-обнаружений отображается информация о количестве обнаружений на устройствах за последний месяц. Виджет доступен для отображения на закладке **Панель мониторинга** в Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console. Из виджета вы можете перейти в раздел **Обнаружения** со списком обнаружений на устройствах.

Чтобы добавить виджет EDR-обнаружений на информационную панель:

1. Перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
3. В списке доступных веб-виджетов выберите веб-виджет **Обнаружения** в категории **Статистика угроз**.
4. Нажмите на кнопку **Добавить**.

Веб-виджет будет добавлен в конец информационной панели.

Подробнее о работе с виджетами см. в *справке Kaspersky Security Center Web Console* или в *справке Kaspersky Security Center Cloud Console*.

Просмотр списка обнаружений

Вы можете просмотреть все обнаружения в виде списка в разделе **Обнаружения** в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

Этот раздел появляется автоматически при [активации решения Kaspersky Endpoint Detection and Response Optimum](#). Вы также можете включить отображение этого раздела в [Kaspersky Security Center Web Console](#)  или [Kaspersky Security Center Cloud Console](#) .

Из списка обнаружений вы можете перейти в [детали выбранного обнаружения](#).

Проверка работоспособности Kaspersky Endpoint Detection and Response Optimum на устройствах

Функциональность Kaspersky Security Center позволяет получить информацию о текущем статусе защиты на устройствах и о том, на каких устройства в вашей инфраструктуре не установлена EPP-программа с поддержкой Kaspersky Endpoint Detection and Response Optimum.

Вы можете получить эту информацию, построив выборку устройств по статусу компонента EDR Optimum.

Чтобы построить выборку устройств по статусу компонента EDR Optimum:

1. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Устройства** → **Выборки устройств**.
2. Создайте новую [выборку устройств](#) со следующим условием:
 - a. Выберите раздел **Информация о программах "Лаборатории Касперского"**.
 - b. В списке **Компоненты программы** выберите компонент **Endpoint Detection and Response** для EPP-программ, установленных на ваших устройствах.
 - c. В раскрывающемся списке **Статус** выберите необходимое значение критерия выборки, чтобы отобразить устройства с этим статусом работы Kaspersky Endpoint Detection and Response Optimum на устройстве.
 - d. Нажмите на кнопку **Сохранить**.

Новая выборка отобразит список устройств с выбранным статусом работы Kaspersky Endpoint Detection and Response Optimum.

Просмотр информации о срабатывании правил запрета запуска

Функциональность Kaspersky Security Center позволяет получить информацию о программах, запуск которых был заблокирован решением Kaspersky Endpoint Detection and Response Optimum в результате срабатывания правила [запрета запуска объектов](#).

Чтобы просмотреть отчет о программах, запуск которых был запрещен:

1. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. В списке отчетов выберите нужный отчет:
 - **Отчет о запрещенных программах** - чтобы просмотреть информацию о программах, запуск которых был запрещен в режиме блокирования и записи в отчет.

- **Отчет о запрещенных программах в тестовом режиме** – чтобы просмотреть информацию о программах, запуск которых был запрещен в режиме только записи событий в отчет.

Получение списка изолированных устройств

Функциональность Kaspersky Security Center позволяет получить информацию об устройствах, к которым была применена [сетевая изоляция](#).

Вы можете получить эту информацию, построив выборку устройств по тегу ISOLATED FROM NETWORK.

Чтобы построить выборку устройств, изолированных от сети:

1. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Устройства** → **Выборка устройств**.
2. Создайте новую [выборку устройств](#)  со следующим условием:
 - a. Выберите раздел **Теги**.
 - b. Нажмите на кнопку **Добавить** и создайте условие выборки всех устройств, обозначенных тегом ISOLATED FROM NETWORK.

Новая выборка отобразит список устройств, изолированных от сети.

Мультитенантность

Режим multitenancy – это режим работы, при котором решение используется для защиты инфраструктуры нескольких организаций одновременно.

Вы можете использовать Kaspersky Endpoint Detection and Response Optimum для защиты инфраструктуры нескольких организаций одновременно с помощью Kaspersky Security Center. Для этого вам требуется в рамках физического Сервера администрирования организации-провайдера создать виртуальные Серверы администрирования организаций, для защиты которых вы хотите использовать Kaspersky Endpoint Detection and Response Optimum. Подробнее о создании виртуальных Серверов администрирования см. в [Справке Kaspersky Security Center](#) .

Для каждой [организации-тенанта](#)  необходимо создать отдельный виртуальный Сервер администрирования. Администратор физического Сервера администрирования может управлять решением на всех устройствах, которые управляются этим Сервером. Администратор виртуального Сервера администрирования может управлять решением только на устройствах, подключенных к Серверу, который он администрирует.

Поддержка мультитенантности в Kaspersky Endpoint Detection and Response Optimum имеет ряд ограничений:

- В Kaspersky Security Center Web Console и в Kaspersky Security Center Cloud Console построить [выборку изолированных устройств](#) на физическом Сервере администрирования можно только после того, как на нем хотя бы раз была применена сетевая изоляция.
- В Kaspersky Security Center Cloud Console:
 - Распределение прав возможно только для учетных записей, зарегистрированных через Active Directory.
 - Права администратора для организации-тенанта необходимо назначить до создания виртуального Сервера администрирования. После создания виртуального Сервера добавить или удалить учетную запись администратора невозможно.
 - Администраторам виртуальных Серверов администрирования доступны права чтения на физическом Сервере.

Источники информации о программе

Страница Kaspersky Endpoint Detection and Response Optimum на веб-сайте "Лаборатории Касперского"

На [странице Kaspersky Endpoint Detection and Response Optimum](#)  вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Endpoint Detection and Response Optimum в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На [странице Kaspersky Endpoint Detection and Response Optimum 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 Detection and Response Optimum, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

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 Kaspersky Endpoint Detection and Response Optimum, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Endpoint Detection and Response Optimum.

Kaspersky предоставляет поддержку Kaspersky Endpoint Detection and Response Optimum в течение жизненного цикла (см. [страницу жизненного цикла программ](#)). Прежде чем обратиться 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](#) .

Глоссарий

Endpoint Protection Platform (EPP)

Интегрированная система комплексной защиты конечных устройств (например, мобильных устройств, компьютеров или ноутбуков) с помощью различных технологий безопасности. Пример Endpoint Protection Platform – программа Kaspersky Endpoint Security для бизнеса.

EPP-программа

Программа, входящая в состав системы защиты конечных устройств (англ. [Endpoint Protection Platform, EPP](#) ). EPP-программы устанавливаются на конечные устройства внутри ИТ-инфраструктуры организации (например, мобильные устройства, компьютеры или ноутбуки). Примером EPP-программы является Kaspersky Endpoint Security для Windows в составе EPP-решения Kaspersky Endpoint Security для бизнеса.

IOС

Indicator of Compromise (индикатор компрометации). Набор данных о вредоносном объекте или действии.

IOC-файл

Файл, содержащий набор индикаторов IOC, при совпадении с которыми программа считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

OpenIOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий свыше 500 различных индикаторов компрометации.

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами сети Интернет.

Действие по реагированию

Действие по реагированию на инцидент – это структурированная методология обработки инцидентов и нарушений системы безопасности и киберугроз.

Тенант

Тенант – это организация, которой предоставляется решение Kaspersky Endpoint Detection and Response Optimum.

Трассировка

Отладочное выполнение программы, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

Целевая атака

Атака, направленная на конкретного человека или организацию. В отличие от массовых атак компьютерными вирусами, направленных на заражение максимального количества компьютеров, целевые атаки могут быть направлены на заражение сети определенной организации или даже одного сервера в IT-инфраструктуре организации. Для каждой целевой атаки может быть написана специальная троянская программа.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory, Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.