kaspersky

Kaspersky Private Security Network

Руководство администратора

Версия программы: 3.3

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 27.11.2021

https://www.kaspersky.ru
https://support.kaspersky.ru

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

kaspersky

Содержание

kaspersky

Об этом руководстве

Руководство администратора Kaspersky Private Security Network 3.3 (далее "Kaspersky Private Security Network") адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Private Security Network, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Private Security Network.

Вы можете применять информацию в этом руководстве для выполнения следующих задач:

- подготовка к установке и установка Kaspersky Private Security Network;
- настройка и использование Kaspersky Private Security Network.

Также из этого руководства вы можете узнать об источниках информации о программе и способах получения технической поддержки.

В этом разделе

В этом документе

Этот документ содержит следующие разделы:

Источники информации о программе (см. стр. 10)

Этот раздел содержит описание источников информации о программе.

Kaspersky Private Security Network (см. стр. 11)

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Private Security Network, перечень аппаратных и программных требований Kaspersky Private Security Network.

Архитектура программы (см. стр. 19)

Этот раздел содержит описание компонентов Kaspersky Private Security Network и их взаимодействия.

Типовые схемы развертывания программы (см. стр. 26)

Этот раздел содержит информацию о типовых схемах развертывания Kaspersky Private Security Network.

Установка программы (см. стр. 30)

Этот раздел содержит пошаговые инструкции по установке Kaspersky Private Security Network.

Веб-интерфейс Kaspersky Private Security Network (см. стр. 42)

Этот раздел содержит информацию об основных элементах интерфейса программы.

Лицензирование программы (см. стр. 43)

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

АО "Лаборатория Касперского" (см. стр. 111)

Этот раздел содержит информацию об АО "Лаборатория Касперского".

Информация о стороннем коде (см. стр. 113)

Этот раздел содержит информацию о стороннем коде, используемом в программе.

Уведомления о товарных знаках

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком "Пример".

Пример текста	Описание условного обозначения
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком "стрелка".
В командной строке введите текст `help` Появится следующее сообщение: Укажите дату в формате `ДД:ММ:ГГ`.	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

kaspersky

Источники информации о программе

Вы можете получить информацию о Kaspersky Private Security Network из настоящего Руководства администратора Kaspersky Private Security Network и электронной справки. Руководство администратора входит в комплект поставки, с его помощью вы можете установить Kaspersky Private Security Network на серверах локальной сети организации и настроить параметры работы программы, а также получить сведения об основных приемах работы с Kaspersky Private Security Network. Во встроенной справке для Kaspersky Private Security Network вы можете найти информацию о веб-страницах программы: описание параметров, ссылки на описание задач, общие сведения о программе.

kaspersky

Kaspersky Private Security Network

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Private Security Network, перечень аппаратных и программных требований Kaspersky Private Security Network.

В этом разделе

О Kaspersky Private Security Network

Kaspersky Private Security Network – это решение, позволяющее пользователям компьютеров, на которые установлены программы "Лаборатории Касперского" (далее "компьютеры организации"), получать доступ к репутационным базам Kaspersky Security Network (см. раздел "О Kaspersky Security Network" на стр. 13), а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.

Kaspersky Private Security Network разработано для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

- отсутствия подключения локальных рабочих мест к сети Интернет;
- законодательного запрета или требований корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Kaspersky Private Security Network может использоваться со следующими корпоративными программами "Лаборатории Касперского":

- Kaspersky Anti Targeted Attack Platform.
- Kaspersky Embedded Systems Security.
- Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Security for Android™.
- Kaspersky Endpoint Security для Linux.
- Kaspersky Endpoint Security для Mac®.
- Kaspersky Endpoint Security для Windows®.
- Kaspersky Fraud Prevention Clientless Engine.
- Kaspersky Fraud Prevention for Endpoint для Windows.
- Kaspersky Industrial Cyber Security for Network.

- Kaspersky Industrial Cyber Security for Nodes.
- Kaspersky Secure Mail Gateway.
- Kaspersky Security Center.
- Kaspersky Security для Windows Server®.
- Kaspersky Security для виртуальных сред Защита без агента.
- Kaspersky Security для виртуальных сред Легкий агент.
- Kaspersky Security для систем хранения данных.
- Kaspersky Web Filter Software Development Kit.
- Kaspersky Web Traffic Security.

Подробную информацию об использовании Kaspersky Private Security Network с корпоративными программами "Лаборатории Касперского" см. в документации к этим программам.

Вы можете использовать Kaspersky Private Security Network в следующих комплектациях:

- **Стандартная**

  Этот вариант используется, если на всех серверах с компонентами Kaspersky Private Security Network разрешен доступ к серверам "Лаборатории Касперского" для получения пакетов с репутационными базами.

- **С однонаправленным шлюзом**

  Этот вариант используется, если в локальной сети организации запрещен доступ к серверам "Лаборатории Касперского". В этом случае локальная сеть организации разделяется на открытый и категорированный сегменты сети. Взаимодействие между сегментами сети осуществляется с помощью однонаправленного шлюза.

  Открытый сегмент сети – участок локальной сети организации, на котором открыт доступ к серверам "Лаборатории Касперского".

  Категорированный сегмент сети – участок локальной сети организации, на котором запрещен доступ к серверам "Лаборатории Касперского".

  Однонаправленный шлюз – устройство, предназначенное для однонаправленной передачи данных из открытого сегмента сети в категорированный сегмент сети.

- **С прокси-сервером**

  Этот вариант используется, если в локальной сети организации запрещен доступ к серверам "Лаборатории Касперского". В этом случае локальная сеть организации разделяется на открытый и категорированный сегменты сети. Взаимодействие между сегментами сети осуществляется по протоколу TCP (Transmission Control Protocol). Взаимодействие с серверами "Лаборатории Касперского" осуществляется через прокси-сервер с установленным компонентом Proxy.

Комплектация Kaspersky Private Security Network определяется корпоративными требованиями безопасности.

kaspersky

О Kaspersky Security Network

Kaspersky Security Network – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о следующих данных:

- репутации файлов, веб-сайтов и программ;
- категориях файлов, веб-сайтов и программ (например, файл операционной системы, компьютерная игра, веб-сайт категории Для взрослых);
- частоте обнаружения файлов во всех странах мира и о географическом распространении файлов;
- статистике доверия к файлам и веб-сайтам среди пользователей программ "Лаборатории Касперского" во всем мире (Kaspersky Application Advisor);
- отзывах вирусными аналитиками "Лаборатории Касперского" отдельных вирусных записей в локальных базах антивирусных программ (например, изменение оценки объекта с "опасный" на "безопасный").

Данные Kaspersky Security Network используются в программах «Лаборатории Касперского» для следующих целей:

- предоставление актуальной информации об объектах, ещё не в вошедших базы антивирусных программ;
- снижения вероятности ложных срабатываний Анти-Спама;
- блокирования доступа пользователя к вредоносным веб-сайтам;
- блокирования запуска вредоносных файлов на компьютере пользователя;
- ограничения доступа к отдельным категориям файлов и веб-сайтов (например, ограничения запуск файлов или веб-сайтов категории Компьютерные игры в рабочее время).

Если пользователь участвует в Kaspersky Security Network, программа "Лаборатории Касперского", установленная на компьютере пользователя, получает информацию из Kaspersky Security Network, а также отправляет в "Лабораторию Касперского" данные о предположительно опасных объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз Kaspersky Security Network.

Об отличиях Kaspersky Private Security Network от Kaspersky Security Network

В отличие от Kaspersky Security Network, использование Kaspersky Private Security Network позволяет пользователю получать информацию из базы знаний "Лаборатории Касперского" без отправки данных на серверы Kaspersky Security Network со своего компьютера.

Отличия принципов работы Kaspersky Security Network и Kaspersky Private Security Network показаны на схеме ниже.

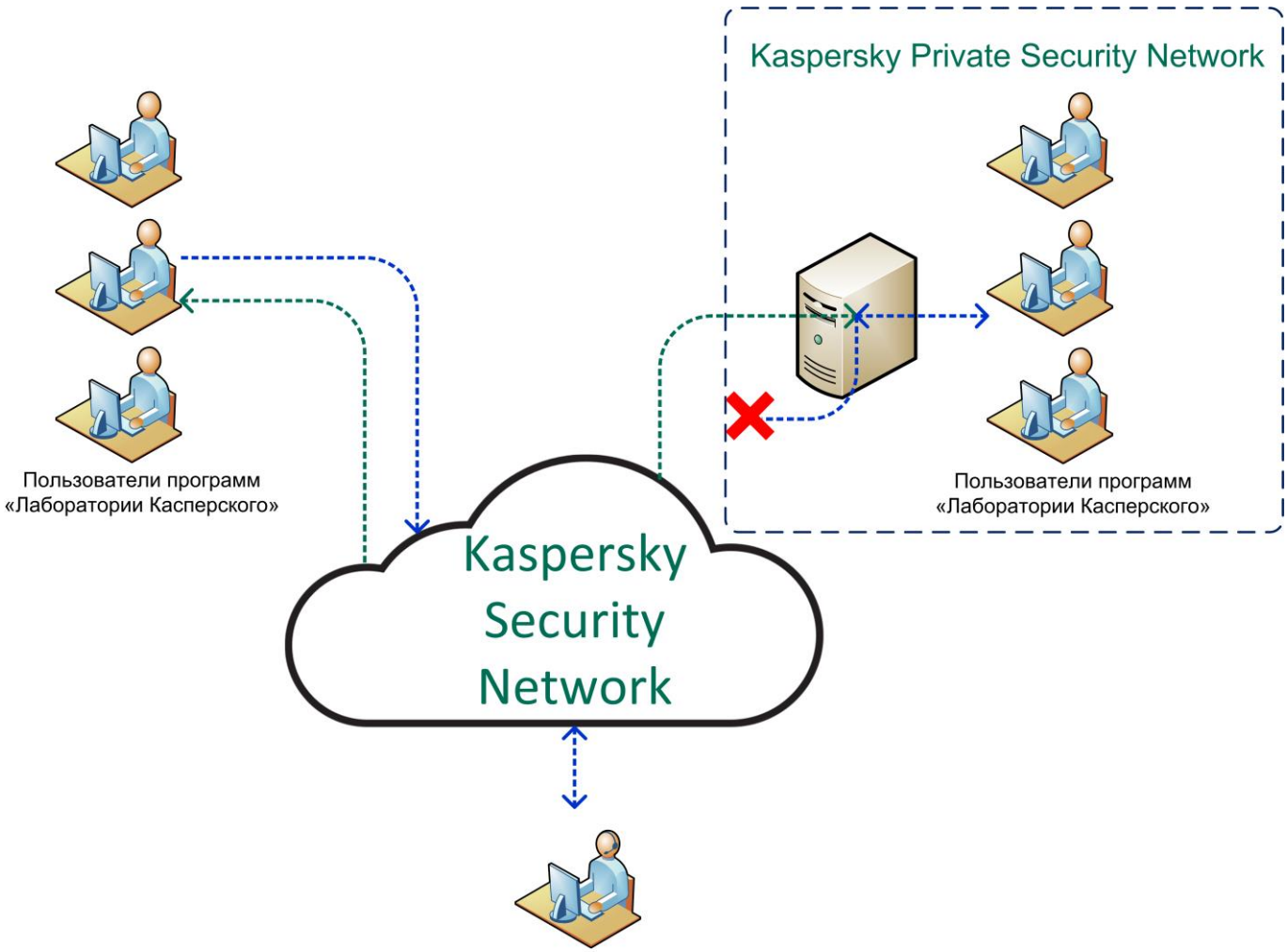


Рисунок 1. Сравнение принципов работы Kaspersky Security Network и Kaspersky Private Security Network

Что нового в версии 3.3

В Kaspersky Private Security Network 3.3 появились следующие возможности и доработки:

- Указаны рекомендуемые требования к надежности паролей.
- Обновлен перечень данных, передаваемых в "Лабораторию Касперского" в рамках запросов на обновление баз (см. раздел "Запрос на обновление баз" на стр. 46).
- Обновлены условия добавления сведений о репутации веб-адресов (см. раздел "Добавление сведений о репутации файла или веб-сайта" на стр. 54) в локальные базы.
- Актуализирован набор параметров, возвращаемых в ответах на API-запросы (см. раздел "Работа с API" на стр. 76) на проверку репутации веб-сайтов или файлов.

kaspersky

Комплект поставки

В комплект поставки Kaspersky Private Security Network входят следующие компоненты:

- TGZ-архив с установочными файлами Kaspersky Private Security Network.
- Руководство администратора Kaspersky Private Security Network.

Состав комплекта поставки может быть различным в зависимости от программ "Лаборатории Касперского", подключаемых к Kaspersky Private Security Network, а также от индивидуальных требований, предъявляемых пользователями Kaspersky Private Security Network.

Аппаратные и программные требования

Вы можете развернуть Kaspersky Private Security Network на серверах под управлением операционной системы Ubuntu. На всех серверах должна быть установлена одинаковая операционная система.

Требования к минимальному количеству серверов для развертывания Kaspersky Private Security Network и аппаратные требования представлены в таблицах ниже. Компоненты Kaspersky Private Security Network устанавливаются в соответствии со схемой развертывания (см. раздел "Типовые схемы развертывания программы" на стр. 26).

Таблица 2. Минимальное количество серверов для развертывания Kaspersky Private Security Network

Комплектация	Серверы	Аппаратные требования
Стандартная	**Сервер 1:** • Monitoring System. • File Reputation. • URL Reputation. • Anti-Spam. • KMP. • Additional Services.	• Процессор – 2,8 ГГц, 16 ядер. • Объем оперативной памяти – 96 ГБ. • Дисковая подсистема – 1 ТБ SSD (не менее 50 000 iops read/write). • Для работы с локальной репутационной базой сервиса FileReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства (см. раздел "Управление локальными репутационными базами" на стр. 52). • Для работы с локальной репутационной базой сервиса UrlReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства и 0,5 ГБ оперативной памяти (см. раздел "Управление локальными репутационными базами" на стр. 52).

Комплектация	Серверы	Аппаратные требования
Стандартная, развертывание на двух серверах	**Сервер 1:** • Monitoring System. • File Reputation. • Anti-Spam.	• Процессор – 2,8 ГГц, 12 ядер. • Объем оперативной памяти – 64 ГБ. • Дисковая подсистема – 1 ТБ SSD (не менее 50 000 iops read/write). • Для работы с локальной репутационной базой сервиса FileReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства (см. раздел "Управление локальными репутационными базами" на стр. 52).
	Сервер 2: • URL Reputation. • KMP. • Additional Services.	• Процессор – 2,8 ГГц, 12 ядер. • Объем оперативной памяти – 64 ГБ. • Дисковая подсистема – 300 ГБ свободного пространства. • Для работы с локальной репутационной базой сервиса UrlReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 1 ГБ дискового пространства и 0,5 ГБ оперативной памяти (см. раздел "Управление локальными репутационными базами" на стр. 52).
С прокси-сервером	**Сервер 1:** • Monitoring System. • File Reputation. • URL Reputation. • Anti-Spam. • KMP. • Additional Services.	• Процессор – 2,8 ГГц, 16 ядер. • Объем оперативной памяти – 96 ГБ. • Дисковая подсистема – 1 ТБ SSD (не менее 50 000 iops read/write). • Для работы с локальной репутационной базой сервиса FileReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства (см. раздел "Управление локальными репутационными базами" на стр. 52). • Для работы с локальной репутационной базой сервиса UrlReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства и 0,5 ГБ оперативной памяти (см. раздел "Управление локальными репутационными базами" на стр. 52).
	Сервер 2: Proxy.	• Не предусмотрено.

Комплектация	Серверы	Аппаратные требования
С прокси-сервером, развертывание на двух серверах	**Сервер 1:** • Monitoring System. • File Reputation. • Anti-Spam.	• Процессор – 2,8 ГГц, 12 ядер. • Объем оперативной памяти – 64 ГБ. • Дисковая подсистема – 1 ТБ SSD (не менее 50 000 iops read/write). • Для работы с локальной репутационной базой сервиса FileReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства (см. раздел "Управление локальными репутационными базами" на стр. 52).
	Сервер 2: • URL Reputation. • KMP. • Additional Services.	• Процессор – 2,8 ГГц, 12 ядер. • Объем оперативной памяти – 64 ГБ. • Дисковая подсистема – 300 ГБ свободного пространства. • Для работы с локальной репутационной базой сервиса UrlReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства и 0,5 ГБ оперативной памяти (см. раздел "Управление локальными репутационными базами" на стр. 52).
	Сервер 3: Proxy.	• Не предусмотрено.
С однонаправленным шлюзом	**Сервер 1:** • Gateway Input. • Monitoring System.	• Процессор – 2 ГГц, 4 ядра. • Объем оперативной памяти – 16 ГБ. • Дисковая подсистема – 16 ГБ свободного пространства.
	Сервер 2: • Gateway Output. • URL Reputation.	• Процессор – 2,8 ГГц, 12 ядер. • Объем оперативной памяти – 64 ГБ. • Дисковая подсистема – 300 ГБ свободного пространства. • Для работы с локальной репутационной базой сервиса UrlReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 1 ГБ дискового пространства и 0,5 ГБ оперативной памяти (см. раздел "Управление локальными репутационными базами" на стр. 52).
	Сервер 3: • Monitoring System. • File Reputation. • Anti-Spam. • KMP. • Additional Services.	• Процессор – 2,8 ГГц, 12 ядер. • Объем оперативной памяти – 96 ГБ. • Дисковая подсистема – 1 ТБ SSD (не менее 50 000 iops read/write). • Для работы с локальной репутационной базой сервиса FileReputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства (см. раздел "Управление локальными репутационными базами" на стр. 52).

Комплектация	Серверы	Аппаратные требования
	Однонаправленный шлюз	• Не предусмотрено.

Требования к сети: сетевой интерфейс с пропускной способностью 100 Мбит/сек.

На серверах Kaspersky Private Security Network хранится конфиденциальная информация (например, журналы работы программы). Рекомендуется обеспечить дополнительную защиту серверов Kaspersky Private Security Network. Например, вы можете разрешить доступ к серверам только по протоколу SSH (Secure Shell). После настройки дополнительной защиты убедитесь, что соединения, необходимые для работы программы, доступны.

Программные требования

- На каждом из серверов, предназначенных для установки компонентов Kaspersky Private Security Network, должна быть установлена операционная система Ubuntu 20.04 Server.
- На серверах должны быть установлены пакеты, перечисленные в Приложении (см. раздел "Список пакетов, необходимых для работы Kaspersky Private Security Network" на стр. 101).
- На компьютере, предназначенном для настройки и работы с Kaspersky Private Security Network через веб-интерфейс, должен быть установлен браузер. Ограничений по использованию типов и версий браузеров Kaspersky Private Security Network не предусмотрено. Рекомендуется использовать браузеры Google™ Chrome™, Mozilla™ Firefox™ или Microsoft® Edge.

kaspersky

Архитектура программы

Архитектура Kaspersky Private Security Network может различаться в зависимости от комплектации программы и операционной системы серверов.

В состав Kaspersky Private Security Network входят следующие компоненты:

- **Gateway Input**

  Компонент Gateway Input (на стр. 23) получает пакеты с репутационными базами от Kaspersky Security Network, проверяет целостность данных, упаковывает данные в файлы и отправляет эти файлы в категорированный сегмент сети.

- **Gateway Output**

  Компонент Gateway Output (на стр. 23) получает файлы с данными из открытого сегмента сети, проверяет целостность и распаковывает их.

- **Proxy**

  Компонент Proxy (на стр. 23) получает пакеты с репутационными базами от Kaspersky Security Network и отправляет эти пакеты в категорированный сегмент сети.

- **File Reputation**

  Компонент File Reputation (на стр. 23) предоставляет программам "Лаборатории Касперского" информацию о репутации и категории файлов.

- **URL Reputation**

  Компонент URL Reputation (на стр. 24) предоставляет программам "Лаборатории Касперского" информацию о репутации и категории веб-сайтов.

- **Anti-Spam**

  Компонент Anti-Spam (на стр. 24) предоставляет программам "Лаборатории Касперского" статистические данные для защиты от спама.

- **Managed Protection (KMP)**

  Компонент KMP (см. раздел "Компонент Managed Protection (KMP)" на стр. 24) предоставляет сервису Kaspersky Managed Protection данные для выявления следов целевых атак, а также своевременного информирования пользователей о возникшей угрозе.

- **Additional Services**

  Компонент Additional Services (на стр. 25) предоставляет программам "Лаборатории Касперского" информацию от вирусных аналитиков "Лаборатории Касперского" о репутации отдельных объектов.

- **Monitoring System**

  Компонент Monitoring System (на стр. 24) позволяет администратору управлять остальными компонентами Kaspersky Private Security Network, а также осуществлять мониторинг работоспособности программы через веб-интерфейс.

  На компьютерах, предназначенных для управления Kaspersky Private Security Network через веб-интерфейс, должен быть установлен браузер. Эти компьютеры должны иметь доступ к серверам с компонентом Monitoring System.

Для обеспечения безопасной передачи данных между Kaspersky Private Security Network и программами в локальной сети организации требуется добавить ключ шифрования трафика (см. раздел "Добавление ключа шифрования трафика" на стр. 36).

Взаимодействие между Kaspersky Private Security Network и Kaspersky Security Network осуществляется по шифрованному каналу с использованием клиентского сертификата для авторизации, который предоставляется заказчику отдельно (см. раздел "Добавление SSL-сертификата" на стр. 38).

Kaspersky Private Security Network работает с операционными системами Linux.

Стандартная комплектация Kaspersky Private Security Network

Архитектура Kaspersky Private Security Network стандартной комплектации представлена на рис. ниже.

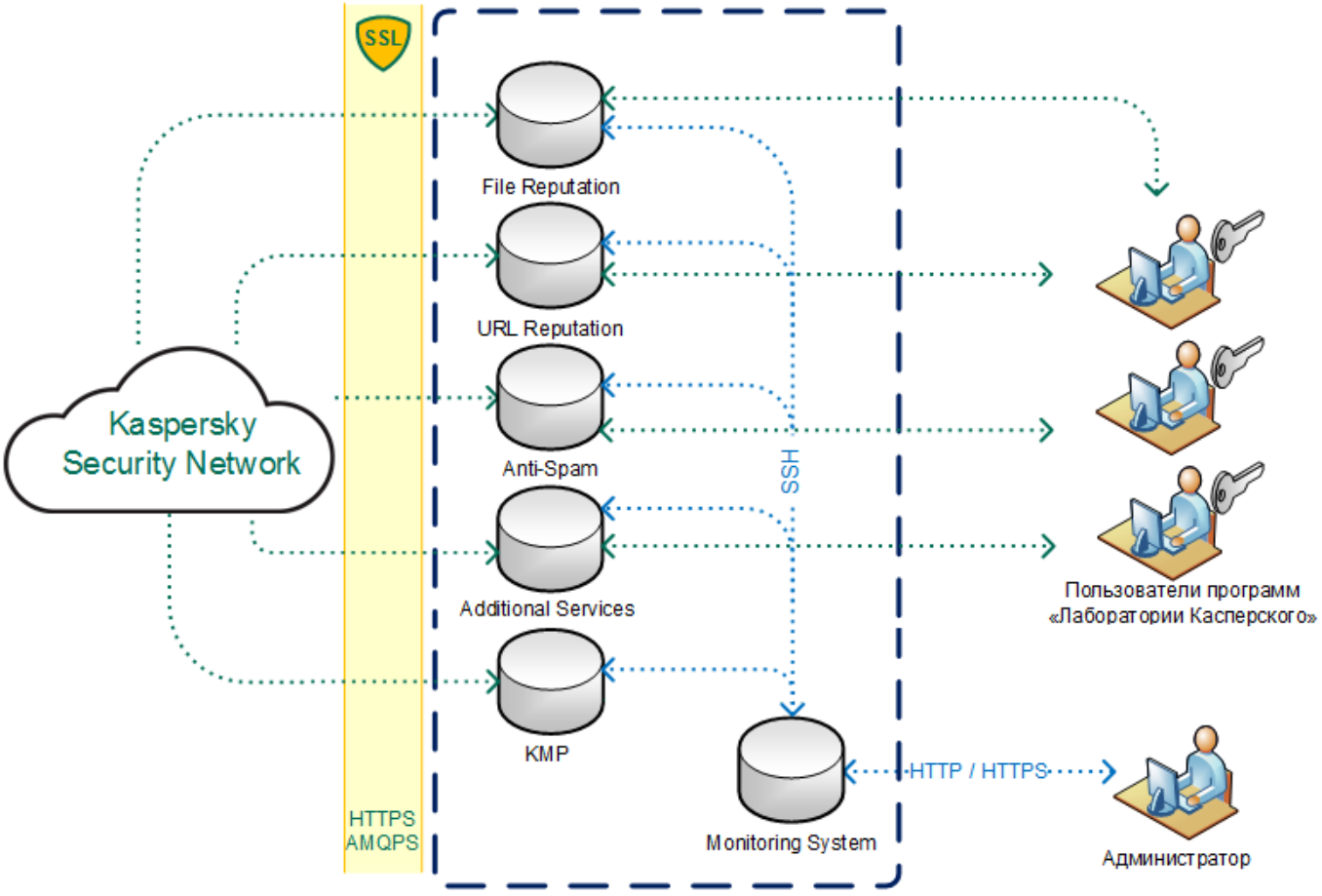


Рисунок 2. Архитектура Kaspersky Private Security Network стандартной комплектации

Kaspersky Private Security Network с однонаправленным шлюзом

Для обеспечения работы однонаправленного шлюза требуется установить компонент Gateway Input в открытом сегменте сети и компонент Gateway Output в категорированном сегменте сети. Для управления Kaspersky Private Security Network требуется установить компонент Monitoring System дважды: в открытом и категорированном сегментах сети.

Архитектура Kaspersky Private Security Network с однонаправленным шлюзом представлена на рис. ниже.

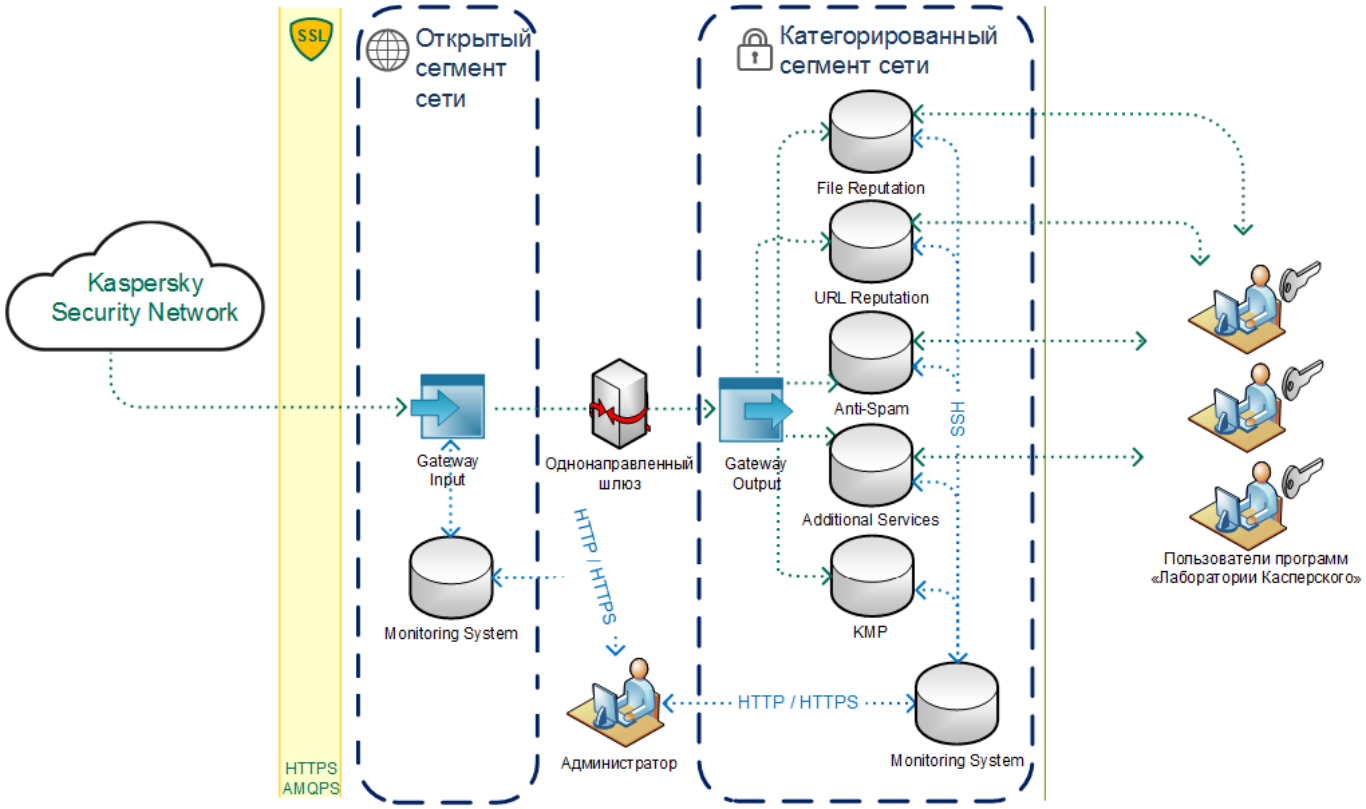


Рисунок 3. Архитектура Kaspersky Private Security Network с однонаправленным шлюзом

Kaspersky Private Security Network с прокси-сервером

Для обеспечения работы прокси-сервера требуется установить компонент Proxy в открытом сегменте сети.

Архитектура Kaspersky Private Security Network с прокси-сервером представлена на рис. ниже.

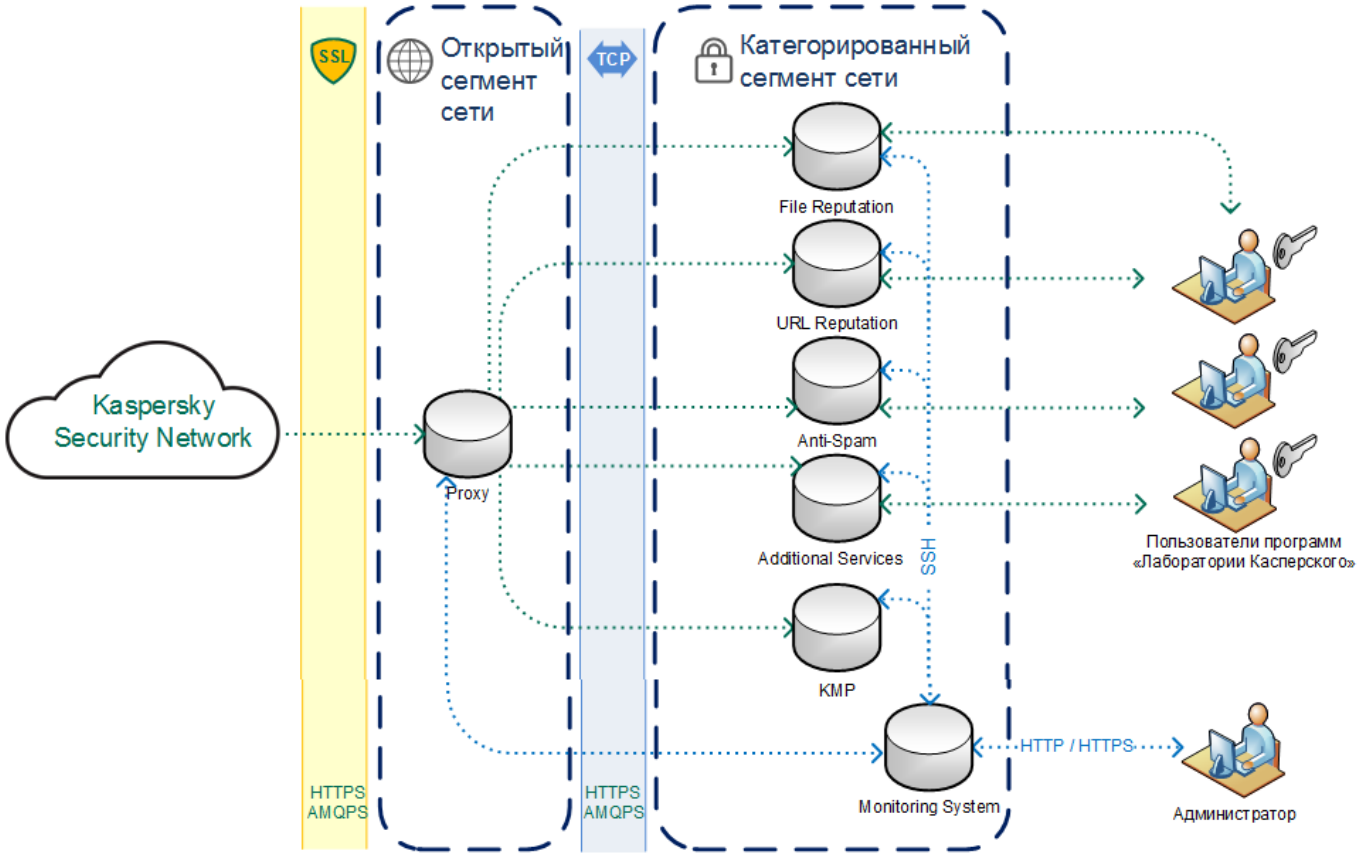


Рисунок 4. Архитектура Kaspersky Private Security Network с прокси-сервером

В этом разделе

Компонент Gateway Input

Компонент Gateway Input устанавливается на сервер в открытом сегменте сети (см. раздел "Установка компонентов Kaspersky Private Security Network" на стр. 35).

Компонент выполняет следующие функции:

- Получение пакетов с репутационными базами для сервисов Kaspersky Private Security Network с серверов "Лаборатории Касперского".
- Проверка целостности принятых данных.
- Упаковка и отправка пакетов с репутационными базами через однонаправленный шлюз в категорированный сегмент сети на сервер с компонентом Gateway Output.

Компонент Gateway Output

Компонент Gateway Output устанавливается на сервер в категорированном сегменте сети (см. раздел "Установка компонентов Kaspersky Private Security Network" на стр. 35).

Компонент выполняет следующие функции:

- Получение упакованных пакетов с репутационными базами через однонаправленный шлюз с сервера с компонентом Gateway Input, расположенного в открытом сегменте сети.
- Проверка целостности принятых данных.
- Обновление репутационных баз сервисов Kaspersky Private Security Network на серверах категорированного сегмента сети.

Компонент Proxy

Компонент Proxy устанавливается на сервер в открытом сегменте сети.

Компонент выполняет следующие функции:

- Получение пакетов с репутационными базами для сервисов Kaspersky Private Security Network с серверов "Лаборатории Касперского".
- Отправка пакетов с репутационными базами по протоколу TCP в категорированный сегмент сети на серверы с установленными компонентами Kaspersky Private Security Network.

Компонент File Reputation

Компонент File Reputation содержит сервис File Reputation.

Сервис File Reputation предоставляет программам "Лаборатории Касперского" информацию о репутации файлов и отображает сведения о категории файла (например, файл операционной системы). Кроме того, сервис предоставляет программам "Лаборатории Касперского" сведения о частоте обнаружения файла во всех странах мира и о географическом распространении файла.

На основании данных сервиса программы "Лаборатории Касперского" могут обнаруживать вредоносные файлы на компьютерах пользователей. Обнаружив вредоносный файл, программа выполняет заданное в параметрах программы действие: лечение, удаление или блокировка. Также на основании данных сервиса программы "Лаборатории Касперского" могут ограничивать запуск отдельных категорий файлов, например, запуск файлов категории Компьютерные игры.

Компонент URL Reputation

Компонент URL Reputation предоставляет сервис URL Reputation.

Сервис URL Reputation

Сервис URL Reputation предоставляет программам "Лаборатории Касперского" информацию о репутации веб-сайтов и отображает сведения о категории веб-сайта (например, Для взрослых).

На основании данных сервиса программы "Лаборатории Касперского" могут блокировать доступ к вредоносным веб-сайтам на компьютерах пользователей и ограничивать доступ к отдельным категориям веб-сайтов.

Компонент Anti-Spam

Компонент Anti-Spam предоставляет сервис Anti-Spam.

Сервис Anti-Spam

Сервис Anti-Spam предоставляет программам защиты почтовых серверов "Лаборатории Касперского" данные для фильтрации почтового потока от нежелательных сообщений (спама). Подробнее о работе программ защиты почтовых серверов см. в документации к этим программам https://help.kaspersky.com/.

Компонент Managed Protection (KMP)

Компонент KMP предоставляет сервису Kaspersky Managed Protection данные для выявления следов целенаправленных атак, а также своевременного информирования пользователей о возникшей угрозе. Полученные данные анализируются в автоматическом режиме, а также вручную специалистами службы мониторинга "Лаборатории Касперского". При этом Kaspersky Private Security Network не передает данные за пределы локальной сети организации, а сохраняет данные внутри локальной сети. Специалисты службы мониторинга "Лаборатории Касперского" должны иметь доступ к этим данным. Полученные данные также могут использоваться в ходе расследования инцидентов. Подробнее о сервисе Kaspersky Managed Protection см. на сайте "Лаборатории Касперского" https://www.kaspersky.com.au/enterprise-security/cybersecurity-services.

Компонент Monitoring System

Компонент Monitoring System позволяет администратору Kaspersky Private Security Network выполнять

следующие действия через веб-интерфейс:

- Удаленно устанавливать компоненты Kaspersky Private Security Network на серверы и управлять ими (см. раздел "Установка компонентов Kaspersky Private Security Network" на стр. 35).
- Осуществлять мониторинг работоспособности Kaspersky Private Security Network, следить за быстродействием и качеством работы сервисов (см. раздел "Мониторинг работы Kaspersky Private Security Network" на стр. 59).
- Управлять учетными записями администраторов Kaspersky Private Security Network (см. раздел "Управление учетными записями администраторов" на стр. 71).
- Осуществлять администрирование локальных репутационных баз File Reputation и URL Reputation.

Если вы используете Kaspersky Private Security Network с однонаправленным шлюзом, компонент Monitoring System устанавливается дважды: на сервер в открытом сегменте сети и на сервер в категорированном сегменте сети (см. раздел "Установка компонента Monitoring System из TGZ-архива" на стр. 32).

Компонент Additional Services

Компонент Additional Services содержит следующие сервисы:

- Record Management.
- Cloud Information.
- Certificate Validation.

Сервис Record Management

Сервис Record Management предоставляет программам "Лаборатории Касперского" информацию от вирусных аналитиков "Лаборатории Касперского" о репутации отдельных объектов в антивирусных базах программ. Сервис используется для быстрой обработки изменений оценки объектов с "опасная" на "безопасная". Если оценка была изменена, сервис Record Management оперативно обновляет данные в антивирусных базах программ "Лаборатории Касперского".

Сервис Cloud Information

Сервис Cloud Information предоставляет программам "Лаборатории Касперского" информацию о показателях баз данных репутации объектов. В программах "Лаборатории Касперского" может отображаться количество безопасных, опасных и других объектов.

Сервис Certificate Validation

Сервис Certificate Validation предоставляет программам "Лаборатории Касперского" информацию о репутации файла по сертификату, которым он был подписан. Если источник сертификата является доверенным (например, официальный магазин программ), файл тоже считается доверенным.

На основе этой информации программы "Лаборатории Касперского" определяют репутацию подписанных файлов (доверенный или недоверенный).

Типовые схемы развертывания программы

Этот раздел содержит информацию о типовых схемах развертывания Kaspersky Private Security Network.

Схема развертывания Kaspersky Private Security Network определяется количеством программ "Лаборатории Касперского", используемых в вашей организации, планируемой нагрузкой на серверы Kaspersky Private Security Network и требованиями корпоративной безопасности.

В этом разделе

Простая схема развертывания

Kaspersky Private Security Network поставляется в следующих комплектациях:

- Стандартная.
- С прокси-сервером.
- С однонаправленным шлюзом.

Выбор комплектации Kaspersky Private Security Network определяется требованиями безопасности вашей организации.

Стандартная комплектация Kaspersky Private Security Network

Для развертывания стандартной комплектации Kaspersky Private Security Network по простой схеме требуется один сервер:

- **Сервер 1**: Monitoring System, File Reputation, URL Reputation, Anti-Spam, KMP и Additional Services.

Простая схема развертывания стандартной комплектации Kaspersky Private Security Network представлена на рис. ниже.

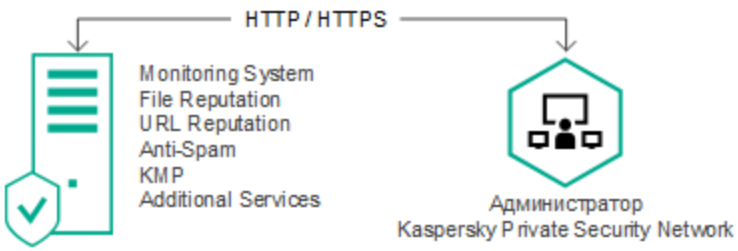


Рисунок 5. Простая схема развертывания стандартной комплектации Kaspersky Private Security Network

Kaspersky Private Security Network с прокси-сервером

Для развертывания Kaspersky Private Security Network с прокси-сервером по простой схеме требуется два сервера:

- Открытый сегмент сети:
  - **Сервер 1**: Proxy.
- Категорированный сегмент сети:
  - **Сервер 2**: Monitoring System, File Reputation, URL Reputation, Anti-Spam, KMP и Additional Services.

Простая схема развертывания Kaspersky Private Security Network с прокси-сервером представлена на рис. ниже.

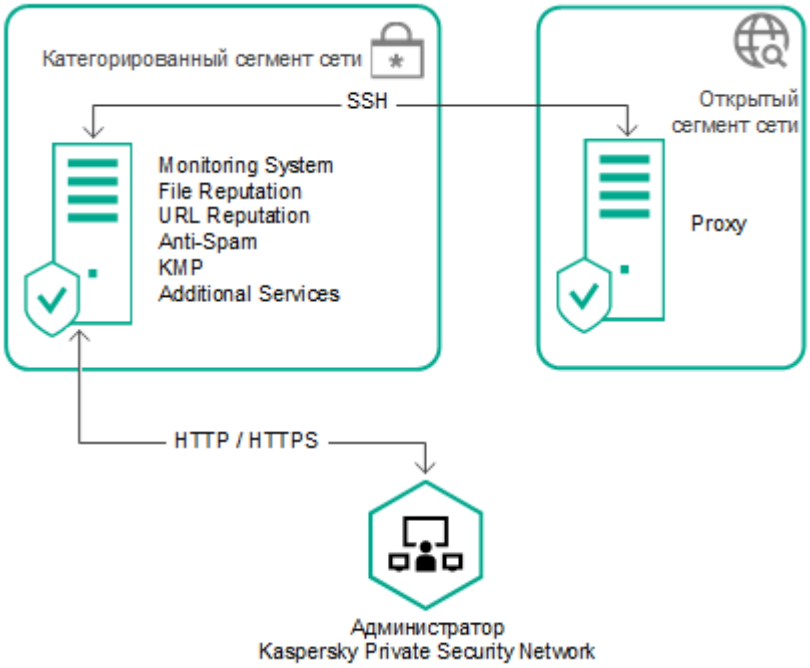


Рисунок 6. Простая схема развертывания Kaspersky Private Security Network с прокси-сервером

Kaspersky Private Security Network с однонаправленным шлюзом

Для развертывания Kaspersky Private Security Network с однонаправленным шлюзом по простой схеме требуется три сервера:

- Открытый сегмент сети:
  - **Сервер 1:** Gateway Input и Monitoring System.
- Категорированный сегмент сети:
  - **Сервер 2:** Gateway Output, URL Reputation, Anti-Spam.
  - **Сервер 3:** Monitoring System, File Reputation, KMP и Additional Services.

Простая схема развертывания Kaspersky Private Security Network с однонаправленным шлюзом представлена на рис. ниже.

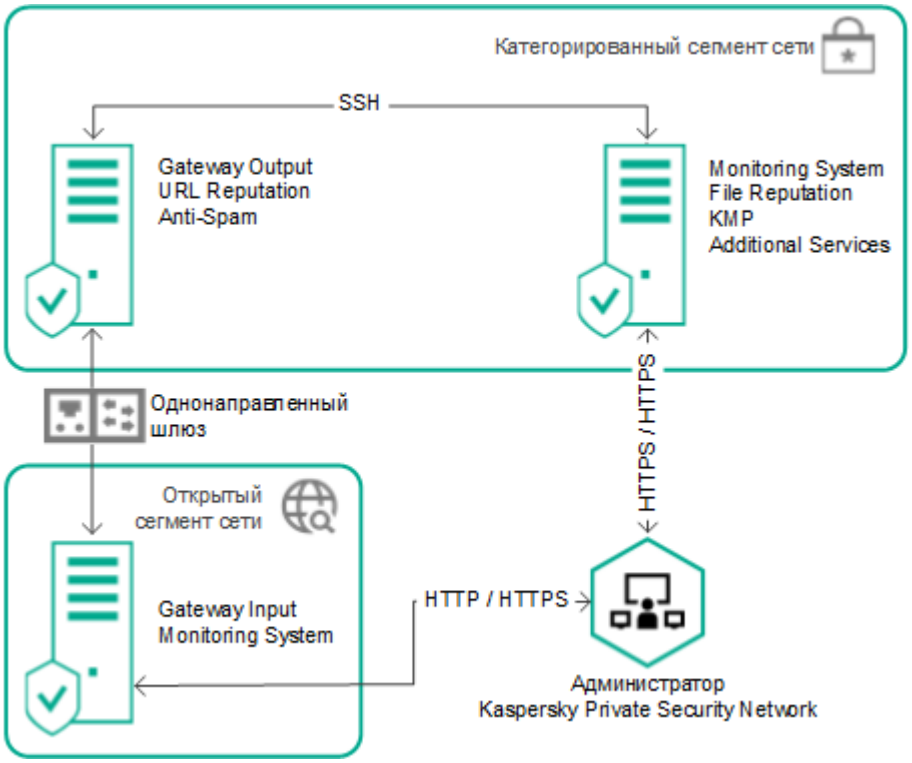


Рисунок 7. Простая схема развертывания Kaspersky Private Security Network с однонаправленным шлюзом

Схема развертывания с резервированием

Вы можете добавить резервные серверы с установленными компонентами Kaspersky Private Security Network для повышения стабильности работы программы. Схема развертывания с резервированием может быть различной в зависимости от корпоративных требований безопасности. Например, вы можете добавить отдельный резервный сервер для компонента URL Reputation.

Добавить резервный сервер для компонентов Monitoring System, Gateway Input, Gateway Output и Proxy невозможно.

Добавление резервного сервера и установка на него компонентов Kaspersky Private Security Network не отличается от добавления основного сервера.

Пример схемы развертывания Kaspersky Private Security Network с резервированием представлен на рис. ниже.

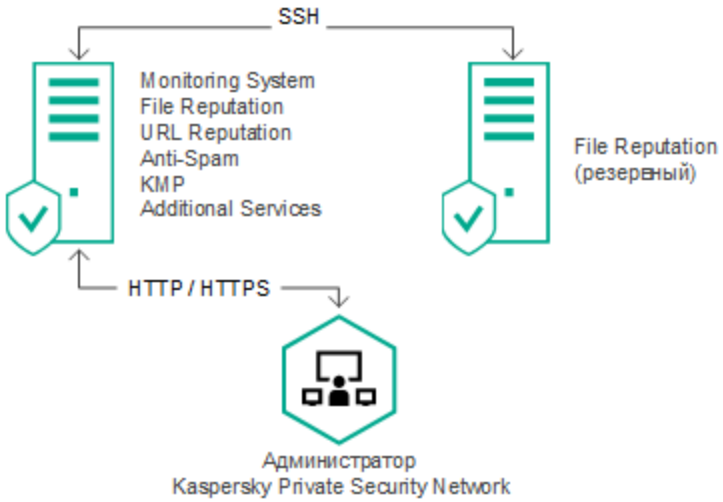


Рисунок 8. Пример схемы развертывания Kaspersky Private Security Network с резервированием

Установка программы

Этот раздел содержит пошаговые инструкции по установке Kaspersky Private Security Network.

Установка Kaspersky Private Security Network состоит из следующих этапов:

1. Установка компонента Monitoring System на сервер.

   Установка производится с помощью установочного скрипта программы, который входит в состав TGZ-архива (см. раздел "Установка компонента Monitoring System из TGZ-архива" на стр. 32).

2. Установка других компонентов Kaspersky Private Security Network.

   Установка производится в веб-интерфейсе программы:

   a. Вход в веб-интерфейс Kaspersky Private Security Network (на стр. 34).

   b. Добавление серверов в веб-интерфейсе программы (см. раздел "Добавление сервера" на стр. 34).

   c. Установка компонентов Kaspersky Private Security Network на серверы (см. раздел "Установка компонентов Kaspersky Private Security Network" на стр. 35).

3. Шифрование трафика между серверами Kaspersky Private Security Network, Kaspersky Security Network и компьютерами с установленными программами "Лаборатории Касперского" (см. раздел "Добавление ключа шифрования трафика" на стр. 36).

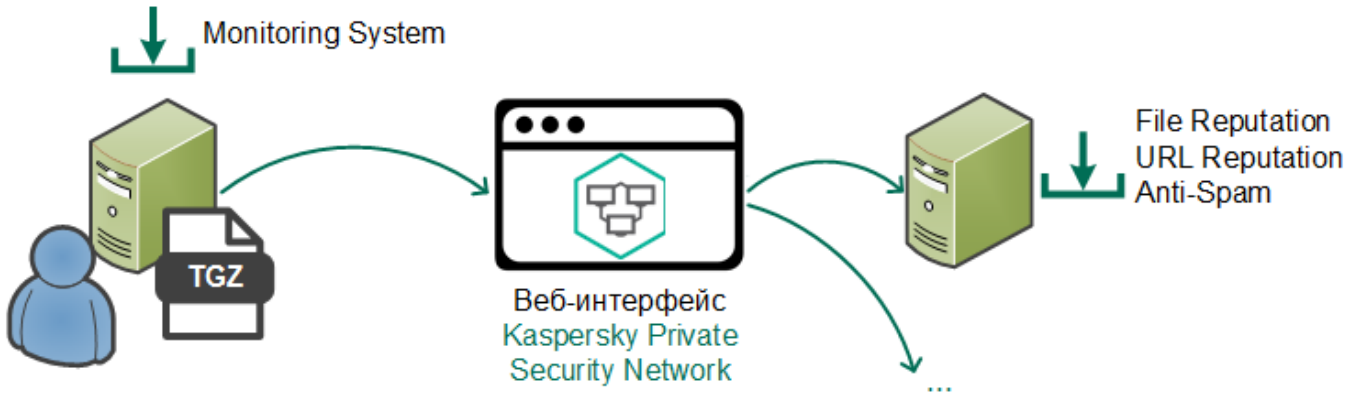


Рисунок 9. Установка компонентов Kaspersky Private Security Network из TGZ-архива и в веб-интерфейсе программы

Вы можете переустанавливать компоненты Kaspersky Private Security Network на другие серверы в веб-интерфейсе программы. Компонент Monitoring System невозможно удалить в веб-интерфейсе программы.

kaspersky

В этом разделе

Подготовка к установке программы

Перед установкой Kaspersky Private Security Network требуется выполнить следующие действия:

1. Убедиться, что серверы находятся внутри локальной сети в соответствии со схемой развертывания (см. раздел "Типовые схемы развертывания программы" на стр. 26).
2. Убедиться, что серверы удовлетворяют аппаратным и программным требованиям (см. раздел "Аппаратные и программные требования" на стр. 15).
3. Убедиться, что разрешены необходимые входящие и исходящие соединения (см. раздел "Список портов для работы программы" на стр. 99).

   Рекомендуется закрыть все порты, кроме перечисленных в разделе Список портов для работы программы (на стр. 99).

4. Если используется Kaspersky Private Security Network с однонаправленным шлюзом, настроить взаимодействие с однонаправленным шлюзом (см. ниже)
5. Убедиться, что операционные системы на серверах, на которые будут установлены компоненты программы, полностью обновлены.

На серверах Kaspersky Private Security Network хранится конфиденциальная информация (например, журналы работы программы). Рекомендуется обеспечить дополнительную защиту серверов Kaspersky Private Security Network. Например, вы можете разрешить доступ к серверам только по протоколу SSH (Secure Shell). После настройки дополнительной защиты убедитесь, что соединения, необходимые для работы программы, доступны.

Добавление пользователя для взаимодействия с компонентами Kaspersky Private Security Network

Для работы с Kaspersky Private Security Network вам требуется добавить пользователя kpsn_system_administrator, имеющего ограниченные привилегии sudo, на все серверы, на которые будут установлены компоненты программы.

► *Чтобы добавить в операционной системе пользователя kpsn_system_administrator:*

1. Запустите скрипт create_kpsn_system_administrator.sh.
2. Задайте и подтвердите пароль для добавляемого пользователя.

Пользователь kpsn_system_administrator будет добавлен в операционную систему.

Вместо пользователя kpsn_system_administrator можно использовать пользователя root, однако для работы программы неограниченные привилегии пользователя root избыточны.

Настройка однонаправленного шлюза при использовании схемы развертывания Kaspersky Private Security Network с однонаправленным шлюзом

Однонаправленный шлюз требуется настроить так, чтобы он передавал файлы из директории /usr/local/ksn/var/zcross_in/<имя потока>/ сервера с компонентом Gateway Input в директорию /usr/local/ksn/var/zcross_out/<имя потока>/ сервера с компонентом Gateway Output, а затем удалял переданные файлы с сервера с компонентом Gateway Input. Структуру вложенных директорий при передаче файлов следует сохранять, поэтому удалять нужно именно файлы, а не директории. Перемещение файлов требуется производить атомарно.

Передаваемые файлы должны иметь права 0666.

Если однонаправленный шлюз поддерживает настройку порядка передачи файлов, рекомендуется передавать их в лексикографическом порядке.

Установка компонента Monitoring System из TGZ-архива

Для установки компонента Monitoring System учетная запись должна обладать правами суперпользователя.

Для Kaspersky Private Security Network с однонаправленным шлюзом установку компонента Monitoring System требуется выполнить дважды: на серверы в открытом и категорированном сегментах сети.

Изменение имени хоста сервера после установки компонентов Kaspersky Private Security Network может привести к сбоям в работе программы.

► *Чтобы установить компонент Monitoring System:*

1. На сервере, предназначенном для компонента Monitoring System, загрузите TGZ-архив с установочным скриптом программы (входит в комплект поставки).
2. Перейдите в директорию, в которую вы загрузили TGZ-архив. Для этого в командной строке введите команду:

```
cd <директория, в которой находится TGZ-архив>
```

3. Распакуйте TGZ-архив. Для этого в командной строке введите команду:

   ```
   tar -xvf <имя TGZ-архива>
   ```

   На сервере будет создана папка, в которую распакуется TGZ-архив.

4. Перейдите в директорию, в которую вы распаковали TGZ-архив. Для этого в командной строке введите команду:

   ```
   cd <директория, в которой распакован TGZ-архив>
   ```

5. Запустите установочный скрипт программы. Для этого в командной строке введите команду:

   ```
   sudo ./kpsn-deb_install
   ```

Компонент Monitoring System будет установлен на сервере.

После установки компонента Monitoring System необходимо добавить сервер с этим компонентом в веб-интерфейсе Kaspersky Private Security Network (см. раздел "Добавление сервера" на стр. 34).

Пример:

```
cd /
tar -xvf kpsn-deb-365.tar.gz
cd /kpsn-deb-365
sudo ./kpsn-deb_install
```

Установка других компонентов в веб-интерфейсе

Установка других компонентов в веб-интерфейсе состоит из следующих этапов:

1. Вход в веб-интерфейс Kaspersky Private Security Network.
2. Добавление серверов в веб-интерфейсе программы.
3. Установка компонентов Kaspersky Private Security Network на серверы.

В этом разделе

kaspersky

Вход в веб-интерфейс Kaspersky Private Security Network

Вы можете войти в веб-интерфейс Kaspersky Private Security Network на любом компьютере, который имеет доступ к серверу с установленным компонентом Monitoring System.

► *Чтобы войти в веб-интерфейс Kaspersky Private Security Network:*

1. В адресной строке браузера введите IP-адрес сервера с установленным компонентом Monitoring System и порт 80 (например, http://10.10.10.10:80).

   Откроется окно ввода учетных данных администратора Kaspersky Private Security Network.

2. Введите учетные данные администратора Kaspersky Private Security Network.

   - **Имя пользователя:** kpsn_admin
   - **Пароль:** RyT;]a8@K)SHw=4f

   > После авторизации с указанными выше учетными данными потребуется изменить пароль администратора (см. раздел "Изменение пароля учетной записи администратора" на стр. 74).

В окне браузера откроется веб-интерфейс Kaspersky Private Security Network. При первом входе в веб-интерфейс программа предлагает вам ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского". Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми пунктами Лицензионного соглашения, примите его. Если вы не согласны с Лицензионным соглашением, вы можете отказаться от него. В этом случае вы не должны использовать Kaspersky Private Security Network.

Добавление сервера

► *Чтобы добавить сервер:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. В панели управления нажмите на кнопку **Добавить сервер**.

   Откроется окно **Добавление сервера**.

4. В поле **Имя** введите имя сервера.
5. В поле **IP/DNS** введите IP-адрес или DNS-имя сервера, на который вы хотите установить компоненты Kaspersky Private Security Network.

   > Для корректной работы Kaspersky Private Security Network рекомендуется использовать IP-адресацию. При установке компонентов Monitoring System (см. раздел "Компонент Monitoring System" на стр. 24) и Gateway Output (см. раздел "Компонент Gateway Output" на стр. 23) можно использовать только IP-адресацию.

Изменение имени хоста сервера после установки компонентов Kaspersky Private Security Network может привести к сбоям в работе программы.

6. В поле **Имя пользователя** и **Пароль** введите данные учетной записи пользователя kpsn_system_administrator (см. раздел "Подготовка к установке программы" на стр. 31).

   Изменить учетную запись пользователя после добавления сервера невозможно.

7. Нажмите на кнопку **Добавить**.

   Сервер будет добавлен в список серверов.

8. Повторите действия пунктов 3–6 для остальных серверов, на которые вы хотите установить компоненты Kaspersky Private Security Network.

Серверы будут добавлены в список серверов.

В рабочей области отображается информация о работе сервера на красном или зеленом фоне:

- **ВКЛ** / **ВЫКЛ** – статус работы компонентов на сервере (запущены / остановлены (см. раздел "Запуск и остановка Kaspersky Private Security Network" на стр. 45)).
- **LOGS** – статус логирования запросов URL Reputation и File Reputation (включено / выключено).
- **RMQ** – статус RabbitMQ™. RabbitMQ позволяет взаимодействовать различным компонентам программы по протоколу AMQP.
- **HTTPD** – статус Apache. Система конфигурации сервера.

Установка компонентов Kaspersky Private Security Network

► *Чтобы установить компоненты Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. В рабочей области выберите сервер, на который вы хотите установить компонент.

   Если сервер для компонента отсутствует в списке, вы можете добавить сервер (см. раздел "Добавление сервера" на стр. 34).

4. Нажмите на кнопку ⭳ рядом с названием компонента Kaspersky Private Security Network.
5. Подтвердите установку компонента по кнопке **ОК**.

   Компонент Kaspersky Private Security Network будет установлен на выбранный сервер.

6. Нажмите на кнопку **Закрыть**.

Информация об установленных компонентах отобразится в описании сервера в списке **Установленные компоненты**.

kaspersky

Шифрование трафика

Данные, передаваемые между серверами Kaspersky Private Security Network, Kaspersky Security Network и компьютерами с установленными программами "Лаборатории Касперского", должны быть зашифрованы. Обеспечение шифрования данных состоит из следующих этапов:

1. Добавление ключа шифрования трафика для безопасного обмена данными между серверами Kaspersky Private Security Network и компьютерами организации. Доступны следующие способы:
   - Создание ключа с помощью Менеджера ключей. Добавление ключа выполняется автоматически.
   - Добавление существующего ключа, созданного сторонним программным обеспечением (например, с помощью пакета OpenSSL).
2. Отправка запроса на использование Kaspersky Private Security Network в "Лабораторию Касперского".
3. Добавление SSL-сертификата для безопасного получения данных от Kaspersky Security Network.

При изменении конфигурации Kaspersky Private Security Network необходимо повторно выполнить процедуры шифрования данных.

В этом разделе

Добавление ключа шифрования трафика

Управление ключами шифрования трафика осуществляется с помощью Менеджера ключей. Менеджер ключей позволяет добавить несколько ключей шифрования трафика в Kaspersky Private Security Network, а также удалить их. Менеджер ключей автоматически назначает каждому ключу шифрования трафика уникальный идентификатор.

Ключ шифрования трафика имеет срок действия 1000 дней.

В Kaspersky Private Security Network ключи шифрования находятся в хранилище ключей шифрования. Вы можете перезаписать хранилище, импортировав, например, хранилище ключей из другого Kaspersky Private Security Network. Вы также можете экспортировать хранилище ключей.

Создание и добавление ключа с помощью Менеджера ключей

► *Чтобы создать ключ шифрования трафика автоматически:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. В панели управления нажмите на кнопку **Менеджер ключей**.

   Откроется окно **Ключи шифрования трафика**.
4. Нажмите на кнопку **Создать ключ**.

Ключ шифрования трафика будет добавлен на все серверы Kaspersky Private Security Network.

Добавление существующего ключа

Вы можете создать закрытый и открытый ключи шифрования трафика вручную, например, с помощью пакета OpenSSL.

> При переустановке Kaspersky Private Security Network закрытый ключ шифрования требуется повторно добавить в веб-интерфейсе программы.

Закрытый ключ должен удовлетворять следующим требованиям:

- длина – 2048 бит;
- кодировка – DER или PEM;
- алгоритм – RSA.

Пример создания ключа с помощью пакета OpenSSL: `openssl genrsa -out private.pem 2048`

► *Чтобы добавить существующий ключ шифрования трафика в Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. В панели управления нажмите на кнопку **Менеджер ключей**.

   Откроется окно **Ключи шифрования трафика**.
4. Нажмите на кнопку **Загрузить ключ**.
5. Выберите файл закрытого ключа.
6. Нажмите на кнопку **Открыть**.

Ключ шифрования трафика будет добавлен на все серверы Kaspersky Private Security Network.

Экспорт и импорт хранилища ключей шифрования трафика

► *Чтобы экспортировать из Kaspersky Private Security Network хранилище ключей шифрования трафика:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. В панели управления нажмите на кнопку **Менеджер ключей**.

   Откроется окно **Ключи шифрования трафика**.
4. Нажмите на кнопку **Экспорт ключей**.

Все ключи из Менеджера ключей Kaspersky Private Security Network будут загружены на ваш компьютер в соответствии с настройками вашего браузера в виде dat-файла хранилища ключей шифрования трафика.

> Если Менеджер ключей пустой, функция экпорта недоступна.

► *Чтобы импортировать в Kaspersky Private Security Network хранилище ключей:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. В панели управления нажмите на кнопку **Менеджер ключей**.

   Откроется окно **Ключи шифрования трафика**.
4. Нажмите на кнопку **Импорт ключей** и в открывшемся окне выберите dat-файл хранилища ключей.
5. Нажмите на кнопку **Открыть**.

Хранилище ключей шифрования трафика будет загружено в Менеджер ключей Kaspersky Private Security Network.

> Импортируемое хранилище ключей шифрования трафика не должно быть пустым. Хотя бы один из содержащихся в хранилище ключей должен иметь действительный срок годности.

> Во время импорта хранилища ключей шифрования трафика ключи, имеющиеся в Менеджере ключей, будут удалены и заменены ключами из загруженного dat-файла.

kaspersky

Добавление SSL-сертификата

Передача данных между Kaspersky Private Security Network и Kaspersky Security Network осуществляется по протоколу HTTPS. Вы получаете архив с SSL-сертификатом в ответном сообщении на запрос в "Лабораторию Касперского", который вы отправили для подтверждения подлинности Kaspersky Private Security Network (см. раздел "Добавление ключа шифрования трафика" на стр. 36).

► *Чтобы добавить SSL-сертификат в Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. В панели управления нажмите на кнопку **Обновить сертификат**.

   Откроется окно выбора файла SSL-сертификата.
4. Выберите архив с SSL-сертификатом (файл в формате TAR.GZ).
5. Нажмите на кнопку **Открыть**.

SSL-сертификат будет автоматически установлен на все серверы Kaspersky Private Security Network.

Вы можете проверить срок действия SSL-сертификата в веб-интерфейсе Kaspersky Private Security Network.

► *Чтобы проверить срок действия SSL-сертификата,*

наведите курсор на кнопку **Обновить сертификат** (см. рис. ниже).

Срок действия SSL-сертификата равен сроку действия лицензии (см. раздел "Лицензирование программы" на стр. 43).
Если почтовые оповещения о проблемах в работе Kaspersky Private Security Network (см. раздел "Получение по почте оповещений об ошибках в работе Kaspersky Private Security Network" на стр. 66) включены, вы будете уведомлены об истечении срока действия SSL-сертификата за 14 дней.

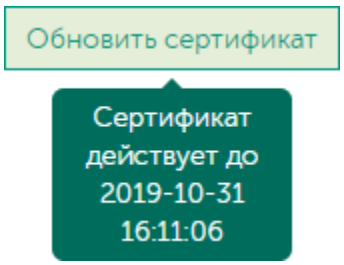


Рисунок 10. Информация о сроке действия сертификата

kaspersky

Отправка запроса в "Лабораторию Касперского"

Для подтверждения подлинности программы вам нужно отправить в "Лабораторию Касперского" запрос на использование Kaspersky Private Security Network. В запрос требуется вложить конфигурационный файл Kaspersky Private Security Network.

Перед отправкой запроса в "Лабораторию Касперского" убедитесь, что все серверы добавлены, компоненты Kaspersky Private Security Network установлены, ключ шифрования трафика добавлен. При изменении конфигурации Kaspersky Private Security Network требуется отправить запрос повторно.

► *Чтобы создать конфигурационный файл Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. В панели управления нажмите на кнопку **Конфигурационный файл**.

   Откроется окно с формой запроса.
4. В поле **Название организации** введите полное название вашей организации, согласованное с "Лабораторией Касперского" (например, "Company_X").

   Используйте следующие символы: a-z, A-Z, 0-9, _ (символ подчеркивания).
5. В поле **Внешние адреса** введите IP-адреса всех серверов, на которых развернут Kaspersky Private Security Network.
6. Нажмите на кнопку **Экспортировать**.

Kaspersky Private Security Network загрузит конфигурационный файл в директорию для загрузки по умолчанию.

В конфигурационный файл, помимо названия вашей организации и внешних IP-адресов серверов Kaspersky Private Security Network, также автоматически включаются следующие сведения: название и версия операционной системы сервера Kaspersky Private Security Network; версия Kaspersky Private Security Network; идентификаторы компонентов Kaspersky Private Security Network, установленных на каждом сервере; CSR (Certificate Signing Request); публичный ключ шифрования трафика.

Вам нужно отправить конфигурационный файл в "Лабораторию Касперского". В ответном сообщении вы получите следующие файлы:

- SSL-сертификат.

  Вам нужно добавить SSL-сертификат в Kaspersky Private Security Network (см. раздел "Добавление SSL-сертификата" на стр. 38).
- Конфигурационные файлы для настройки Kaspersky Private Security Network в других корпоративных программах "Лаборатории Касперского", например, в Kaspersky Security Center.

  Подробнее о работе Kaspersky Private Security Network с другими программами "Лаборатории Касперского" см. в документации к этим программам.

kaspersky

Настройка HTTPS

Взаимодействие между компьютером, на котором открыт веб-интерфейс Kaspersky Private Security Network, и сервером с компонентом Monitoring System по умолчанию осуществляется по протоколу HTTP. Для обеспечения дополнительной защиты при работе Kaspersky Private Security Network вам нужно установить HTTPS-соединение. Для настройки HTTPS вам требуется самостоятельно подготовить сертификат и ключ.

Работа с API осуществляется только по протоколу HTTPS (см. раздел "Работа с API" на стр. 76).

Перед настройкой HTTPS убедитесь, что сервер с компонентом Monitoring System добавлен в веб-интерфейсе Kaspersky Private Security Network (см. раздел "Добавление сервера" на стр. 34).

► *Чтобы настроить HTTPS:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. Нажмите на кнопку **Режимы** → **Monitoring System** → **HTTPS**.

   Откроется окно для добавления сертификата и ключа HTTPS.
4. Выберите ключ от сертификата HTTPS и SSL-сертификат.
5. Нажмите на кнопку **Изменить**.

   Kaspersky Private Security Network потребует ввести учетные данные повторно.
6. В адресной строке браузера измените IP-адрес сервера с установленным компонентом Monitoring System и порт 80 на HTTPS (например, https://10.10.10.10:80).
7. Выполните вход в веб-интерфейс Kaspersky Private Security Network.

Взаимодействие между компьютером, на котором открыт веб-интерфейс Kaspersky Private Security Network, и сервером с компонентом Monitoring System будет осуществляться по протоколу HTTPS.

Веб-интерфейс Kaspersky Private Security Network

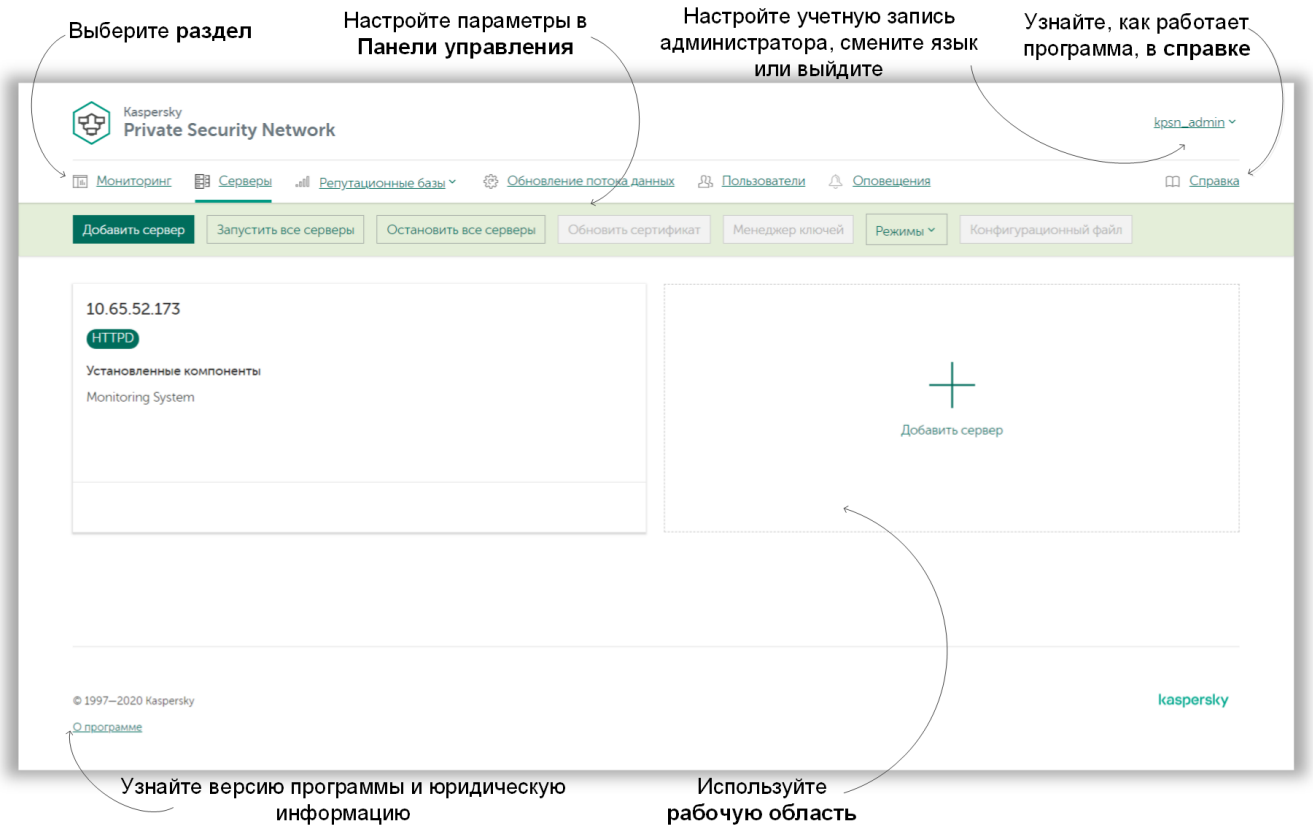


Рисунок 11. Веб-интерфейс Kaspersky Private Security Network

kaspersky

Лицензирование 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.

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- При первом входе в веб-интерфейс Kaspersky Private Security Network.
- На сервере с установленным компонентом Monitoring System в директории /usr/local/ksn/kpsn_panel_2/kpsn_panel_2/files/.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения при первом входе в веб-интерфейс Kaspersky Private Security Network. Если вы не согласны с условиями Лицензионного соглашения, вы не должны использовать программу.

О лицензии

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

Срок действия лицензии равен сроку действия SSL-сертификата (см. раздел "Добавление SSL-сертификата" на стр. 38).

Лицензия включает в себя право на получение следующих услуг:

- Использование программы.
- Обращение в Службу технической поддержки "Лаборатории Касперского".
- Получение прочих услуг, предоставляемых вам "Лабораторией Касперского" или ее партнерами в течение срока действия лицензии.

Функциональность программы, доступная по лицензии, зависит от вида лицензии. Для Kaspersky Private Security Network предусмотрены следующие виды лицензии:

- **Kaspersky Private Security Network Standart**
  - Поддержка до 50 тыс. устройств.
- **Kaspersky Private Security Network Advanced**
  - Поддержка до 500 тыс. устройств.
  - Управление локальными репутационными базами (корпоративные списки разрешенных и запрещенных файлов и адресов).
  - Поддержка модели поставщика услуг (xSP model).
  - Высокая доступность (до 10 узлов с возможностью кластеризации).

Активация программы выполняется автоматически после установки и запуска программы при наличии подключения к интернету.

О Лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с комплектом поставки.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- 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.

Запуск и остановка Kaspersky Private Security Network

► *Чтобы запустить или остановить компоненты Kaspersky Private Security Network на серверах:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. Запустите или остановите Kaspersky Private Security Network следующими способами:
   - Чтобы запустить или остановить все компоненты Kaspersky Private Security Network, в панели управления нажмите на кнопку **Запустить все серверы** или **Остановить все серверы**.
   - Чтобы запустить или остановить компоненты на отдельном сервере:
     a. Выберите сервер, на котором вы хотите запустить или остановить компоненты Kaspersky Private Security Network.
     b. Нажмите на кнопку **Запустить** или **Остановить**.

Информация о состоянии компонентов отображается в рабочей области серверов (**ВКЛ** или **ВЫКЛ**).

kaspersky

Обновление баз

Обновление баз Kaspersky Private Security Network осуществляется по шаблону Publisher-Subscriber (Издатель – Подписчик). *Publisher-Subscriber* – шаблон передачи данных, в котором подписчик автоматически устанавливает соединение с издателем, и после этого получает обновления по защищенному каналу.

Publisher – это издатель и отправитель данных. Издателем выступает "Лаборатория Касперского", отправляющая обновления данных для сервисов Kaspersky Private Security Network.

Subscriber – это подписчик и получатель данных. Подписчиками выступают серверы с сервисами Kaspersky Private Security Network.

В общем случае обновление баз выполняется по следующему алгоритму:

1. Kaspersky Private Security Network на стороне локальной сети вашей организации устанавливает соединение с серверами "Лаборатории Касперского" и отправляет запрос на получение обновлений.

   Запрос может быть выполнен через сервер с компонентом Proxy. Для Kaspersky Private Security Network с однонаправленным шлюзом запрос выполняется вручную (см. раздел "Запуск потока обновления данных вручную" на стр. 50).

2. "Лаборатория Касперского" проверяет базы Kaspersky Security Network на наличие обновлений.
3. При наличии обновлений "Лаборатория Касперского" шифрует поток обновлений баз.
4. "Лаборатория Касперского" отправляет поток обновлений (ответ) на серверы с сервисами Kaspersky Private Security Network.

   Ответ может быть получен через сервер с компонентом Proxy или через однонаправленный шлюз. Для Kaspersky Private Security Network с однонаправленным шлюзом потоки обновлений дополнительно упаковываются в файлы для обмена между компонентами Gateway Input и Gateway Output.

   Вы можете контролировать объем входящего трафика и количество полученных пакетов по графику **Получение репутационных баз** (см. раздел "**Мониторинг качества связи с сервисами Kaspersky Security Network**" на стр. 64).

5. Kaspersky Private Security Network проверяет целостность данных.
6. Kaspersky Private Security Network обновляет базы сервисов.

В этом разделе

kaspersky

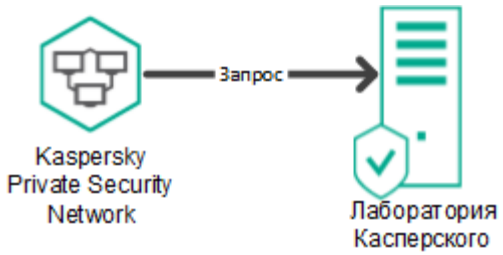
Запрос на обновление баз

Для обновления баз программа отправляет запросы на серверы "Лаборатории Касперского".

Запросы не содержат данных об инфраструктуре организации, компьютерах локальной сети и другой конфиденциальной информации.

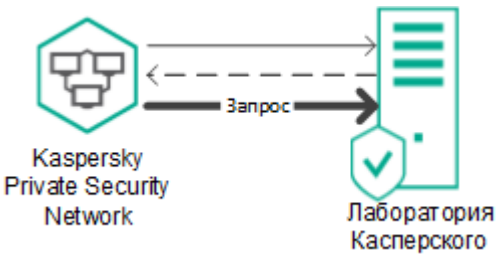
Запрос в "Лабораторию Касперского" содержит следующие данные (используется протокол HTTPS):

- идентификатор установки Kaspersky Private Security Network;
- версия Kaspersky Private Security Network;
- название программы Kaspersky Private Security Network;
- имя, версия и номер сборки операционной системы;
- дата последнего обновления баз;
- признак необходимости подписи для обновлений баз;
- имя потока;
- тип подписи обновления баз.



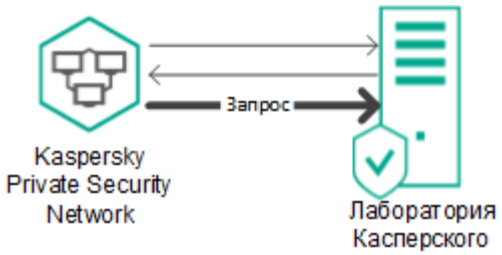
При сбоях в обновлении баз Kaspersky Private Security Network отправляет в "Лабораторию Касперского" дополнительный запрос со следующими данными (используется протокол HTTPS):

- идентификатор установки Kaspersky Private Security Network;
- версия Kaspersky Private Security Network;
- название программы Kaspersky Private Security Network;
- имя, версия и номер сборки операционной системы;
- признак сбоя обновления баз;
- признак необходимости подписи для обновлений баз;
- имя потока;
- признак, является ли запрос мониторингом состояния баз;
- данные о сбое (количество ошибок, их идентификаторы и описания).



После успешного обновления баз Kaspersky Private Security Network отправляет в "Лабораторию Касперского" запрос со следующими данными (используется протокол AMQPS):

- признак успешного обновления.



Алгоритмы обновления баз

Алгоритм обновления баз определяется комплектацией Kaspersky Private Security Network.

Стандартная комплектация Kaspersky Private Security Network

Алгоритм обновления баз в стандартной комплектации Kaspersky Private Security Network представлен на рис. ниже.

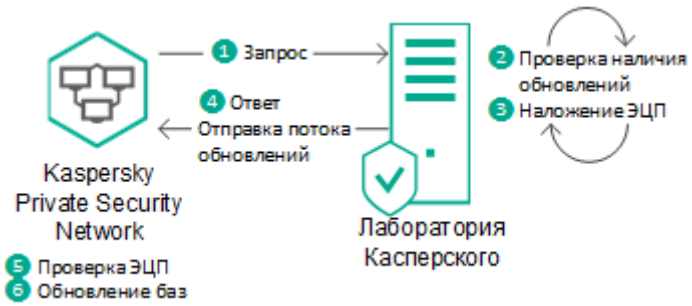


Рисунок 12. Алгоритм обновления баз в стандартной комплектации Kaspersky Private Security Network

Kaspersky Private Security Network с однонаправленным шлюзом

Алгоритм обновления баз в Kaspersky Private Security Network с однонаправленным шлюзом представлен на рис. ниже.

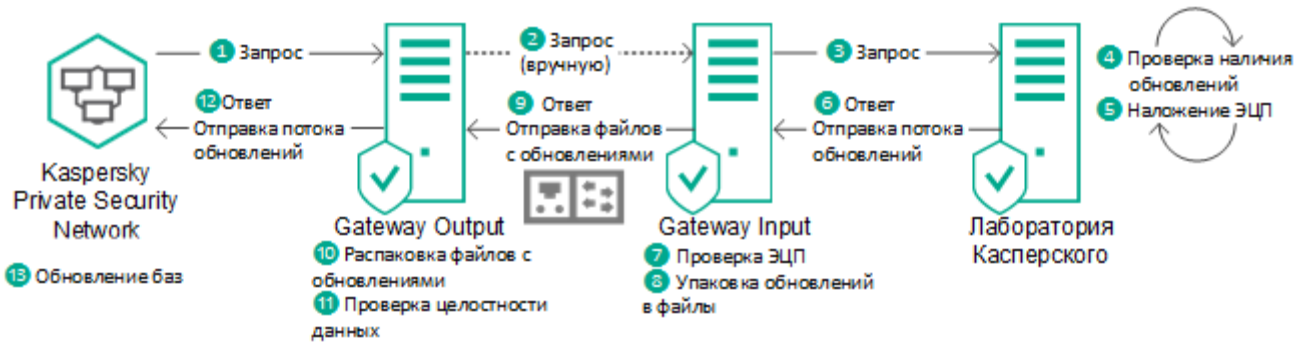


Рисунок 13. Алгоритм обновления баз в Kaspersky Private Security Network с однонаправленным шлюзом

Kaspersky Private Security Network с прокси-сервером

Алгоритм обновления баз в Kaspersky Private Security Network с прокси-сервером представлен на рис. ниже.

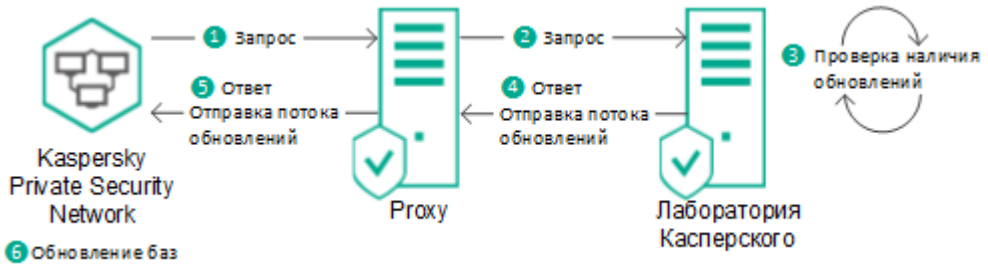


Рисунок 14. Алгоритм обновления баз в Kaspersky Private Security Network с прокси-сервером

Контроль обновления баз

Вы можете контролировать обновление баз Kaspersky Security Network для устранения сбоев при обновлении данных. Если обновление потока завершилось с ошибкой, Kaspersky Private Security Network повторит попытку обновления автоматически.

► *Чтобы контролировать обновление баз:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Обновление потока данных**.
3. Нажмите на кнопку **Обновить данные**, чтобы актуализировать данные.

Отобразится таблица с потоками данных, которые были обновлены в Kaspersky Private Security Network (см. рис. ниже).

Сервер	Время ↑	ID потока	ID пакета	Описание	Статус
10.65.52.220	2018-11-14 07:36:39	CloudInfo	6EFBA6B4-7D7F-43D0-91B8-42BB1FD041FB		OK
10.65.52.220	2018-11-14 07:36:40	MobileCertRep	3E3686A9-C5E6-4077-AFFB-86E50D0052F6		OK
10.65.52.220	2018-11-14 07:36:43	MobileCertRep	14B8AAB3-9880-4FD7-8E00-062D5E81CF0F		OK
10.65.52.220	2018-11-14 07:36:44	MobileCertRep	CEA8F34E-3CB3-457F-B23F-925235DDE218		OK
10.65.52.220	2018-11-14 07:36:44	RMS	43868DE3-DB3D-44AB-ADB1-CB88D6283C5D		OK
10.65.52.220	2018-11-14 07:36:46	RMS	E58CAC54-3D1C-4B3D-A97A-419F9590F4D7		OK
10.65.52.220	2018-11-14 07:36:47	MobileCertRep	E0638188-3E7A-4110-8B96-EF4E1301E795		OK
10.65.52.220	2018-11-14 07:36:48	RMS	C942C66D-AC19-4904-8EA4-DA0E31526218		OK
10.65.52.220	2018-11-14 07:36:50	RMS	85468680-B578-4746-B459-12C9D8418C16		OK
10.65.52.220	2018-11-14 07:36:51	MobileCertRep	1A7EB370-E733-4D14-ADBC-2449A905A7AD		OK

Показать 10 записей на странице (46 всего) 1 2 3 Далее →

Рисунок 15. Контроль обновления баз

kaspersky

Запуск потока обновления данных вручную

Если вы используете Kaspersky Private Security Network с однонаправленным шлюзом, вы можете управлять потоками обновления данных для всех сервисов. По умолчанию все потоки обновления данных остановлены.

► *Чтобы запустить потоки обновления данных:*

1. Откройте веб-интерфейс категорированного сегмента сети Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. Нажмите на значок рядом с IP-адресом сервера с установленным компонентом Gateway Output.

   Откроется окно **Статус потоков данных** с доступными для запуска потоками данных.
4. Запишите или сохраните идентификаторы потоков данных, которые вы хотите запустить.
5. Откройте веб-интерфейс открытого сегмента сети Kaspersky Private Security Network в окне браузера.
6. Выберите раздел **Серверы**.
7. Нажмите на значок рядом с IP-адресом компонента Gateway Input.

   Откроется окно **Обновление потока данных**.
8. Выберите поток данных, который вы хотите запустить:
   - В раскрывающемся списке слева выберите сервис, поток данных которого вы хотите запустить.
   - В поле справа введите идентификатор потока данных, полученный в п. 4.
9. Нажмите на кнопку **Обновить**.
10. Повторите действия пунктов 8–9 для всех потоков обновления данных, которые вы хотите запустить.

    Потоки обновлений данных будут загружены на сервер категорированного сегмента сети.

kaspersky

Выбор режима работы File Reputation

Kaspersky Private Security Network загружает пакеты с репутационными базами файлов для работы сервиса File Reputation. Файлы в пакетах определены хешем: SHA256 или MD5. В зависимости от типа и версии программы "Лаборатории Касперского" используют для определения репутации файлов базы с SHA256 или MD5. Для экономии ресурсов выберите режим работы File Reputation: загружать пакеты только с базами SHA256 или только с базами MD5. Более новые программы поддерживают базы с SHA256. Вы можете просмотреть тип баз File Reputation, используемых программами "Лаборатории Касперского", в документации к этим программам.

► *Чтобы выбрать режим работы File Reputation:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. Нажмите на кнопку **Режим** → **File Reputation**.
4. В выпадающем меню выберите режим работы сервиса File Reputation: **MD5** или **SHA256**.

   Откроется окно подтверждения смены режима работы сервиса File Reputation.
5. Нажмите на кнопку **Изменить**.

Kaspersky Private Security Network будет загружать пакеты с репутационными базами файлов в соответствии с выбранным режимом.

kaspersky

Управление локальными репутационными базами

Kaspersky Private Security Network позволяет гибко использовать данные сервисов File Reputation и URL Reputation с помощью локальных репутационных баз.

Локальная репутационная база – база данных репутаций объектов (файлов или веб-адресов), которая хранится на сервере с установленными компонентами Kaspersky Private Security Network, а не на серверах Kaspersky Security Network. Управление локальными репутационными базами осуществляется администратором Kaspersky Private Security Network (см. раздел "Настройка разрешений" на стр. 72). Данные локальных репутационных баз доступны только для компьютеров организации.

Репутация объекта в локальной репутационной базе имеет приоритет выше, чем в Kaspersky Security Network. То есть, если в локальной репутационной базе объект имеет репутацию *недоверенный*, а в Kaspersky Security Network объект имеет репутацию *доверенный*, то для пользователей сети организации объект будет иметь репутацию *недоверенный* (см. рис. ниже).

Порядок работы с локальными репутационными базами

Управление локальными репутационными базами должно осуществляется одновременно не более чем одним администратором по следующему алгоритму:

1. Администратор Kaspersky Private Security Network выбирает файл или веб-сайт, данные о которых требуется добавить или изменить в локальной репутационной базе.
2. Администратор Kaspersky Private Security Network присваивает объекту одно из следующих значений репутации: доверенный или недоверенный.
3. Kaspersky Private Security Network отображает данные, полученные о репутации объекта, в базах Kaspersky Security Network, если они есть. Также программа отображает сведения о репутации объекта, которую администратор Kaspersky Private Security Network назначил ранее.
4. Администратор Kaspersky Private Security Network принимает окончательное решение о репутации объекта и добавляет или изменяет данные в локальной репутационной базе.
5. Программы "Лаборатории Касперского", использующиеся в вашей организации, получают обновленные данные о репутации объекта.

Лучшие практики присвоения репутации программам

Обычно, чтобы запретить или разрешить запуск программ достаточно функций программ "Лаборатории Касперского" – *Контроль программ*. Контроль программ позволяет настроить доступ к категориям программ (например, играм) или отдельным программам по метаданным или другим данным. В результате запуск программы будет заблокирован. Подробную информацию о работе Контроля программ см. в *документации к программам "Лаборатории Касперского"*.

Вы также можете использовать локальные репутационные базы Kaspersky Private Security Network, чтобы запретить или разрешить запуск программ. Если вы используете Kaspersky Private Security Network, программы с репутацией *недоверенный* будут удалены, а не заблокированы. Также использование локальных репутационных баз имеет ряд особенностей (см. ниже). Например, программы "Лаборатории Касперского" не запрашивают в Kaspersky Security Network / Kaspersky Private Security Network репутацию программ, подписанных доверенным сертификатом Microsoft. Таким образом, репутация программ, которую вы задали в Kaspersky Private Security Network, не влияет на их работу.

Если вы используете собственные программы, не подписанные доверенным сертификатом, вам нужно присвоить таким программам репутацию *доверенный*. Присвоение программе репутации *доверенный* состоит из следующих этапов:

1. Добавьте сведения о собственной программе в локальную репутационную базу.
2. В параметрах программ "Лаборатории Касперского" добавьте категорию программ: KL-категория / Другие программы / Программы, доверенные согласно репутации в KSN.
3. В параметрах Контроля программ разрешите запуск программ из новой категории.

Особенности использования локальных репутационных баз

Kaspersky Private Security Network может использоваться с разными программами "Лаборатории Касперского" (см. раздел "О Kaspersky Private Security Network" на стр. 11). Определение репутации объектов из локальных репутационных баз может отличаться в зависимости от программы "Лаборатории Касперского", установленной на компьютерах организации. Например, определение репутации объекта программой может отличаться по следующим причинам:

- Программы "Лаборатории Касперского" используют *офлайн репутационные базы*. Офлайн репутационные базы включают в себя базы доверенных программ (*Microsoft System Critical Application*), доверенных сертификатов (*Trusted Certificate*) и другие данные. Офлайн репутационные базы предназначены для оптимизации ресурсов при работе программ "Лаборатории Касперского" и защите критически важных объектов компьютера. Офлайн репутационные базы формируют специалисты "Лаборатории Касперского" на основании данных Kaspersky Security Network. Программы "Лаборатории Касперского" обновляют офлайн репутационные базы с антивирусными базами программы. Если информация об объекте содержится в офлайн репутационных базах, то программа не запрашивает репутацию этого объекта в Kaspersky Security Network / Kaspersky Private Security Network.
- В параметрах программы настроены исключения из проверки (доверенная зона). В этом случае программа не учитывает репутацию объекта в Kaspersky Private Security Network.
- Программа использует технологии оптимизации проверки, например, технологии iSwift, iChecker или кеширование запросов репутации в Kaspersky Security Network / Kaspersky Private Security Network. В этом случае программа может не запрашивать репутацию проверенных объектов.
- Программа запрашивает репутацию файлов только определенных форматов.
- Программа не запрашивает репутацию файлов больших размеров.
- Программа запрашивает репутацию объекта в определенных случаях. Например, программа запрашивает репутацию исполнительных файлов при запуске и не запрашивает при проверке файла по расписанию.

Подробную информацию об особенностях использования локальных репутационных баз с корпоративными программами "Лаборатории Касперского" см. в документации к этим программам.

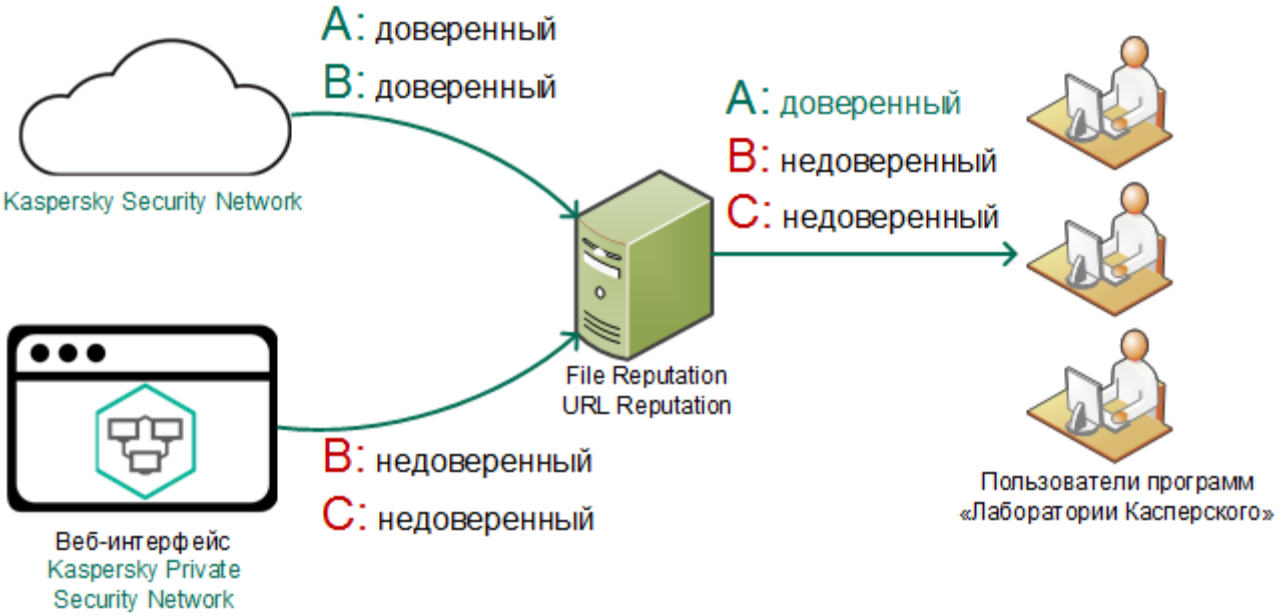


Рисунок 16. Схема работы администратора Kaspersky Private Security Network с локальными репутационными базами

В этом разделе

Добавление сведений о репутации файла или веб-сайта

Kaspersky Anti Targeted Attack Platform позволяет добавлять сведения о репутации файлов и веб-сайтов автоматически. В этом случае объектам присваивается статус *Недоверенный*. Подробнее см. в *Руководстве администратора Kaspersky Anti Targeted Attack Platform*.

► *Чтобы добавить сведения о репутации файла в локальную репутационную базу:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. В панели управления выберите раздел **Репутационные базы → File Reputation**.
3. Нажмите на кнопку **Добавить** и выберите способ добавления файла:

- **Ввести хеш**.

  Вы можете дополнительно ввести имя файла и его описание.

- **Загрузить список хешей из файла**.

  В этом случае необходимо предварительно создать файл с расширением txt и добавить в него список хешей (MD5 или SHA256). Рекомендуется добавлять не более 1000 записей в один файл.

  Вы можете дополнительно ввести имя файла (не более 256 символов) и его описание (не более 1024 символов) после знака табуляции (например, `1BC29B36F623BA82AAF6724FD3B16718 file name description`). Каждая запись должна начинаться с новой строки.

- **Загрузить файл**.

  Вы можете дополнительно ввести описание файла.

4. Выберите репутацию, которую вы хотите присвоить файлу или всем файлам, если вы загружаете список из файла с расширением txt:
   - **Доверенный**.
   - **Недоверенный**.
5. Нажмите на кнопку **Сохранить**.

   Откроется окно Контроля соответствия.
6. Сравните сведения о репутации файла, добавленные в локальную базу ранее, и сведения из базы Kaspersky Security Network (KL-репутация). Примите решение о том, какую репутацию следует присвоить этому файлу.
7. Нажмите на кнопку **Сохранить**.

Новые сведения о репутации выбранного файла будут доступны для программ "Лаборатории Касперского", использующихся в вашей организации.

► *Чтобы добавить сведения о веб-сайте в локальную репутационную базу:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. В панели управления выберите раздел **Репутационные базы → URL Reputation**.
3. Нажмите на кнопку **Добавить** и выберите способ добавления файла:
   - **Ввести URL**.

     Вы можете дополнительно ввести описание веб-сайта.

   - **Загрузить список URL из файла**.

     В этом случае необходимо предварительно создать файл с расширением txt и добавить в него список URL. Рекомендуется добавлять не более 1000 записей URL в один файл.

     Вы можете дополнительно ввести описание веб-сайта (не более 1024 символов) после знака табуляции (например, `example.com description`). Каждая запись должна начинаться с новой строки.

   URL должны удовлетворять требованию RFC 3986, допускается использование маски (*).

Вводите URL без префикса `www`. Программы "Лаборатории Касперского" при запросе репутации в Kaspersky Security Network / Kaspersky Private Security Network не учитывают префикс `www`. Если в локальную репутационную базу добавлен веб-сайт `www.example.com`, то программы "Лаборатории Касперского" не определят репутацию веб-сайта `example.com`.

4. Выберите репутацию, которую вы хотите присвоить веб-сайту или всем веб-сайтам, если вы загружаете список из файла с расширением txt:
   - **Доверенный**.
   - **Недоверенный**.
5. Нажмите на кнопку **Сохранить**.

   Откроется окно Контроля соответствия.
6. Сравните сведения о репутации веб-сайта, добавленные в локальную базу ранее, и сведения из базы Kaspersky Security Network (KL-репутация). Примите решение о том, какую репутацию следует присвоить этому веб-сайту.
7. Нажмите на кнопку **Сохранить**.

Новые сведения о репутации выбранного веб-сайта будут доступны для программ "Лаборатории Касперского", использующихся в вашей организации.

Контроль соответствия сведений о репутации файла или веб-сайта

После обновления репутационных баз Kaspersky Security Network может появиться несоответствие новых сведений о репутации объекта (файла или веб-сайта) данным локальной репутационной базы. Вы можете изменить или подтвердить репутацию объекта в локальной базе после обновления баз Kaspersky Security Network.

Если сведения о репутации объекта содержатся в базе Kaspersky Security Network и в локальной репутационной базе, Kaspersky Private Security Network использует данные из локальной репутационной базы.

► *Чтобы обновить сведения о репутации объекта в локальной репутационной базе:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. В панели управления выберите раздел **Репутационные базы**.
   - Чтобы обновить сведения о репутации файлов, выберите пункт **File Reputation**.
   - Чтобы обновить сведения о репутации веб-сайтов, выберите пункт **URL Reputation**.
3. В панели управления нажмите на кнопку **Контроль соответствия**.

   Откроется список объектов, репутация которых в локальной базе не соответствует репутации в обновленных базах Kaspersky Security Network.

4. Сравните сведения о репутации объекта и примите решение о том, какую репутацию следует присвоить этому объекту.
5. Нажмите на кнопку **Сохранить**.

Сведения об объекте будут обновлены в локальной репутационной базе. Обновленные сведения о репутации объекта будут доступны для программ "Лаборатории Касперского", использующихся в вашей организации.

Экспорт локальной репутационной базы в текстовый файл

► *Чтобы экспортировать данные из локальной репутационной базы:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. В панели управления выберите раздел **Репутационные базы**:
   - Если вы хотите экспортировать сведения о репутации файлов, выберите пункт **File Reputation**.
   - Если вы хотите экспортировать сведения о репутации веб-сайтов, выберите пункт **URL Reputation**.
3. Нажмите на кнопку **Экспорт**:
   - Если вы хотите экспортировать сведения о доверенных объектах, выберите пункт **Доверенные**.
   - Если вы хотите экспортировать сведения о недоверенных объектах, выберите пункт **Недоверенные**.

Kaspersky Private Security Network загрузит файл со списком доверенных или недоверенных объектов в директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах вашего браузера.

Удаление сведений о репутации файла

► *Чтобы удалить сведения о файле из локальной репутационной базы:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. В панели управления выберите раздел **Репутационные базы** → **File Reputation**.
3. Нажмите на кнопку **Удалить** и выберите способ удаления файла:
   - **Ввести хеш**.
   - **Загрузить список хешей из файла**.

     В этом случае необходимо предварительно создать файл с расширением txt и добавить в него список Hash (MD5 и SHA256). Каждая запись должна начинаться с новой строки.
   - **Загрузить файл**.
4. Нажмите на кнопку **Удалить**.

Сведения о файле будут удалены из локальной репутационной базы. Сведения о репутации файла будут недоступны для программ "Лаборатории Касперского", использующихся в вашей организации.

► *Чтобы удалить сведения о веб-сайте из локальной репутационной базы:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. В панели управления выберите раздел **Репутационные базы** → **URL Reputation**.
3. Нажмите на кнопку **Удалить** и выберите способ удаления файла:
   - **Ввести URL**.
   - **Загрузить список URL из файла**.

     В этом случае необходимо предварительно создать файл с расширением txt и добавить в него список URL. Каждая запись должна начинаться с новой строки.
4. Нажмите на кнопку **Удалить**.

Сведения о веб-сайте будут удалены из локальной репутационной базы. Сведения о репутации веб-сайта будут недоступны для программ "Лаборатории Касперского", использующихся в вашей организации.

kaspersky

Мониторинг работы Kaspersky Private Security Network

Этот раздел содержит информацию о мониторинге работы Kaspersky Private Security Network в веб-интерфейсе.

В этом разделе

Мониторинг трафика между программами "Лаборатории Касперского" и Kaspersky Private Security Network

► *Чтобы просмотреть объем входящего и исходящего трафика между сервисами Kaspersky Private Security Network и программами "Лаборатории Касперского":*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Мониторинг**.
3. В раскрывающемся списке серверов выберите сервер, информацию о котором вы хотите просмотреть.

   Если вы хотите просмотреть информацию о всех серверах, выберите вариант **Все серверы**.
4. В раскрывающемся списке комплексных экранов мониторинга Kaspersky Private Security Network выберите вариант **Трафик от программ**.
5. В раскрывающемся списке временных интервалов выберите интервал, за который вы хотите просмотреть информацию о работе сервисов.

На комплексном экране отобразятся графики для каждого из сервисов Kaspersky Private Security Network (см. рис. ниже).

Входящий трафик

По графику вы можете контролировать следующие параметры:

- Объем входящего трафика к сервисам Kaspersky Private Security Network от программ "Лаборатории Касперского" в секунду – область графика, заполненная синим цветом.

- Количество запросов к сервисам Kaspersky Private Security Network от программ "Лаборатории Касперского" в секунду – линия зеленого цвета.

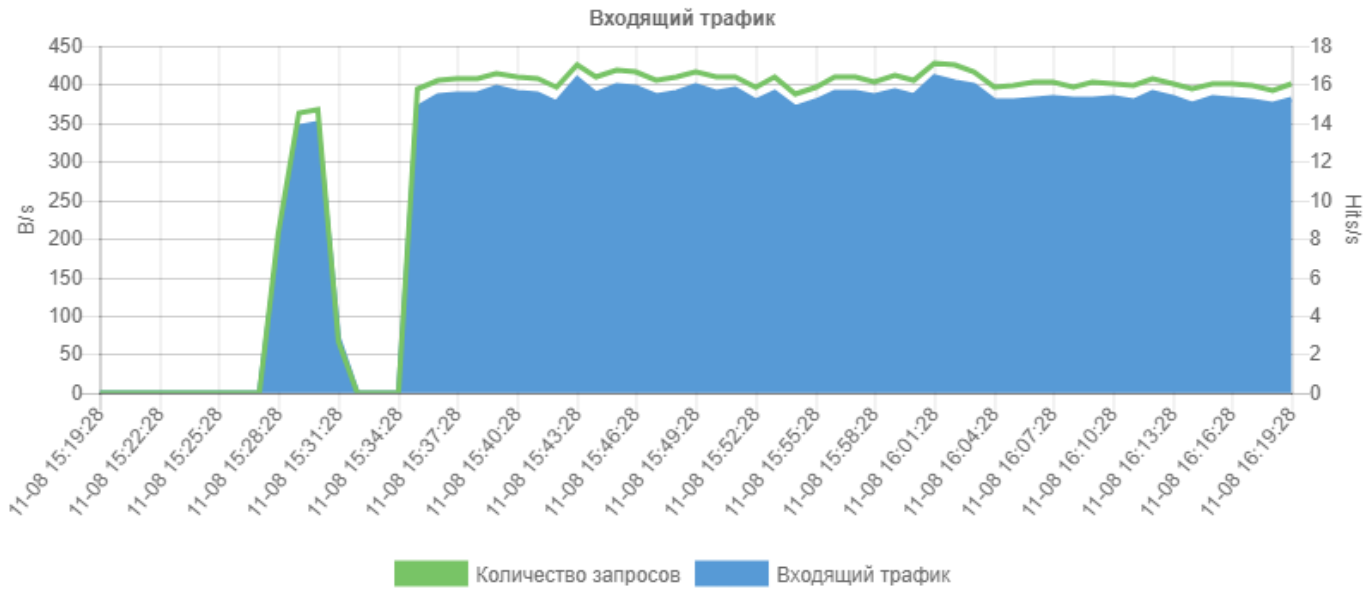


Рисунок 17. График входящего трафика

Исходящий трафик

По графику вы можете контролировать объем исходящего трафика от сервисов Kaspersky Private Security Network к программам "Лаборатории Касперского" в секунду.

Рисунок 18. График исходящего графика

Отображаются графики и диаграммы с общими данными, не разделенными по сервисам или потокам.

Мониторинг работоспособности сервисов Kaspersky Private Security Network

► *Чтобы контролировать работоспособность сервисов Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Мониторинг**.
3. В раскрывающемся списке серверов выберите сервер, информацию о котором вы хотите просмотреть.

   Если вы хотите просмотреть информацию о всех серверах, выберите вариант **Все серверы**.
4. В раскрывающемся списке комплексных экранов мониторинга Kaspersky Private Security Network выберите вариант **Входящие запросы**.
5. В раскрывающемся списке временных интервалов выберите интервал, за который вы хотите просмотреть информацию о работе сервисов.

На комплексном экране отобразятся графики для каждого из сервисов Kaspersky Private Security Network (см. рис. ниже).

Скорость обработки запросов

По графикам вы можете контролировать количество запросов к сервисам Kaspersky Private Security Network от программ "Лаборатории Касперского" и быстродействие обработки этих запросов:

- Если область графика заполнена зеленым цветом, запросы обрабатываются менее чем за 2 сек. Это показатель нормальной работы Kaspersky Private Security Network.
- Если область графика заполнена черным цветом, запросы обрабатываются с задержкой до 10 сек.
- Если область графика заполнена оранжевым цветом, запросы обрабатываются более 10 сек.
- Если область графика заполнена красным цветом, запросы не обрабатываются.
- Если область графика заполнена голубым цветом, версия Kaspersky Private Security Network устарела. Запросы не обрабатываются. Требуется обновить программу.

Графики доступны в виде столбчатой диаграммы для контроля количества запроса по датам и круговой диаграммы для контроля соотношения скоростей обработки запросов за выбранный период.

Рисунок 19. График количества запросов от программ "Лаборатории Касперского" к сервисам Kaspersky Private Security Network

Состав отображаемых графиков и диаграмм соответствует подключенным сервисам (см. стр. 19).

Мониторинг репутации объектов

► *Чтобы просмотреть статистику ответов от сервисов Kaspersky Private Security Network на запросы программ "Лаборатории Касперского":*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Мониторинг**.
3. В раскрывающемся списке серверов выберите сервер, информацию о котором вы хотите просмотреть.

   Если вы хотите просмотреть информацию о всех серверах, выберите вариант **Все серверы**.
4. В раскрывающемся списке комплексных экранов мониторинга Kaspersky Private Security Network выберите вариант **Ответы компьютерам локальной сети**.
5. В раскрывающемся списке временных интервалов выберите интервал, за который вы хотите просмотреть информацию о работе сервисов.

На комплексном экране отобразятся графики для каждого из сервисов Kaspersky Private Security Network (см. рис. ниже).

Репутация ответов (статистика)

По графику вы можете контролировать количество ответов о хорошей / плохой / неизвестной репутации объектов от сервисов Kaspersky Private Security Network, а также локальной репутационной базы, в секунду.

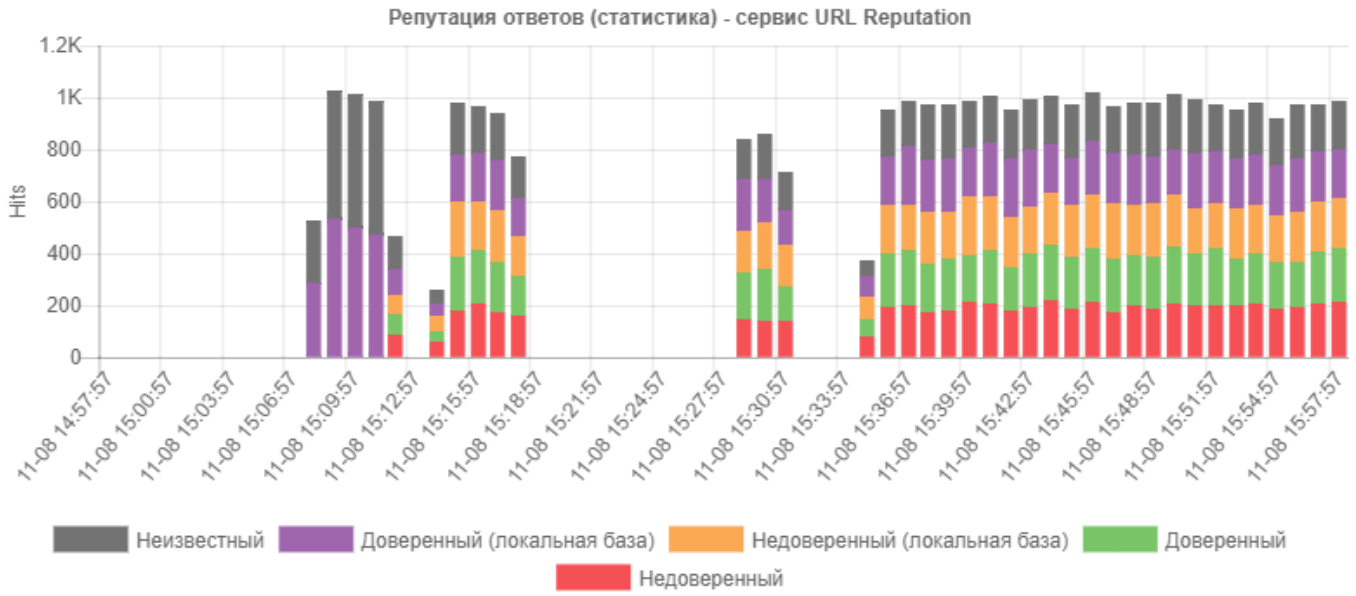


Рисунок 20. График репутации объектов

Репутация ответов (круговая диаграмма)

С помощью диаграммы вы можете контролировать процентное отношение ответов об объектах с хорошей / плохой / неизвестной репутацией к общему числу ответов от сервисов Kaspersky Private Security Network, а также локальной репутационной базы.

Рисунок 21. Диаграмма репутации объектов

Отображаются графики и диаграммы только для сервисов File Reputation и URL Reputation (см. стр. 19).

Мониторинг качества связи с сервисами Kaspersky Security Network

► *Чтобы контролировать качество связи между сервисами Kaspersky Private Security Network и Kaspersky Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Мониторинг**.
3. В раскрывающемся списке серверов выберите сервер, информацию о котором вы хотите просмотреть.

   Если вы хотите просмотреть информацию о всех серверах, выберите вариант **Все серверы**.
4. В раскрывающемся списке комплексных экранов мониторинга Kaspersky Private Security Network выберите вариант **Обновление баз KSN**.
5. В раскрывающемся списке временных интервалов выберите интервал, за который вы хотите просмотреть информацию о работе сервисов.

На комплексном экране отобразятся графики для каждого из сервисов Kaspersky Private Security Network (см. рис. ниже).

Получение репутационных баз

По графику вы можете контролировать следующие параметры:

- Объем входящего трафика с репутационными базами от Kaspersky Security Network к сервисам Kaspersky Private Security Network в секунду – область графика, заполненная синим цветом.
- Количество пакетов с репутационными базами от Kaspersky Security Network к сервисам Kaspersky Private Security Network в секунду – линия зеленого цвета.

Рисунок 22. График объема входящего графика с репутационными базами

Время с момента предыдущего обновления

По графику вы можете контролировать отставание локальных репутационных баз от баз Kaspersky Security Network. Если вы установили несколько одинаковых компонентов Kaspersky Private Security Network на разные серверы (например, установлен резервный сервер с компонентом URL Reputation), по графику вы можете сравнивать отставание в получении пакетов между одинаковыми сервисами. Для этого в списке серверов требуется выбрать вариант **Все серверы**:

- Красным цветом на графике отображается максимальное отставание локальных репутационных баз от баз Kaspersky Security Network на одном из серверов.
- Синим цветом на графике отображается минимальное отставание локальных репутационных баз от баз Kaspersky Security Network на одном из серверов. Или в Kaspersky Private Security Network установлен только один компонент.
- Зеленым цветом на графике отображается среднее значение отставания локальных репутационных баз от баз Kaspersky Security Network.

Рисунок 23. График отставания локальных баз от баз Kaspersky Security Network

Состав отображаемых графиков и диаграмм зависит от режима работы Kaspersky Private Security Network и подключенных потоков данных.

Мониторинг статуса компонентов Kaspersky Private Security Network

Kaspersky Private Security Network автоматически проверяет статус своих компонентов (см. раздел "Архитектура программы" на стр. 19), контролируя следующие параметры:

- доступность необходимого ПО для системы мониторинга Zabbix;
- актуальность ключей шифрования трафика и сертификатов на обновление данных;
- доступность серверов по SSH;
- статус активных процессов Kaspersky Private Security Network на каждом сервере;

- отставание баз по каждому из потоков на каждом сервере;
- качество обработки запросов каждым сервисом на каждом из серверов.

► *Чтобы узнать статус компонентов Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Мониторинг**.
3. Нажмите на кнопку **Общий статус**.

Откроется окно **Общий статус** с таблицей выполненных проверок и их результатов. Дата и время последней проверки указаны в верхнем левом углу окна.

Получение по почте оповещений об ошибках в работе Kaspersky Private Security Network

► *Чтобы получать оповещения об ошибках в работе компонентов Kaspersky Private Security Network по электронной почте:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Оповещения**.
3. В блоке параметров **Оповещения по электронной почте** задайте параметры почтового оповещения:
   a. В поле **Адрес почтового сервера** укажите адрес почтового сервера вашей организации (например, `smtp.example.com`).
   b. В поле **Порт почтового сервера** укажите порт почтового сервера вашей организации (например, `25`).
   c. Если вы хотите использовать TLS-протокол, установите флажок **Использовать TLS**.

      Чтобы использовать протокол TLS, предварительно вам требуется убедиться, что на сервере Kaspersky Private Security Network добавлен доверенный сертификат почтового сервера.
      Если вы включили использование протокола TLS, почтовые оповещения пересылаются с помощью агента отправки электронной почты (MSA, mail submission agent). При этом протокол SMTPS не поддерживается.

   d. В полях **Имя пользователя** и **Пароль** введите имя и пароль учетной записи администратора Kaspersky Private Security Network.
   e. В поле **Отправитель** введите адрес электронной почты или имя, которые будут указаны в качестве отправителя почтового оповещения.
   f. В поле **Получатели** введите адрес электронной почты получателя оповещений. Можно указать несколько адресов, разделяя их точкой с запятой.
   g. Нажмите на кнопку **Получить код подтверждения**.

На каждый адрес электронной почты, указанный в поле **Получатели**, будет отправлено сообщение с общим для всех получателей кодом подтверждения.

h. В поле **Код подтверждения** введите код подтверждения и нажмите на кнопку **Проверить**, чтобы подтвердить адрес электронной почты получателя.

i. Установите флажок **Оповещать о новых проблемах в работе компонентов программы**, чтобы получать оповещения при возникновении ошибок в работе компонентов Kaspersky Private Security Network.

j. Установите флажок **Высылать регулярные оповещения о статусе компонентов программы**, чтобы получать ежедневную рассылку о существующих ошибках в работе компонентов Kaspersky Private Security Network.

k. Нажмите на кнопку **Сохранить**.

Оповещения об ошибках в работе Kaspersky Private Security Network будут включены.

Добавление в Syslog сведений об ошибках в работе Kaspersky Private Security Network

► *Чтобы добавлять в Syslog сведения об ошибках в работе компонентов Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Оповещения**.
3. В блоке параметров **Оповещения Syslog** установите флажки напротив типов ошибок, сведения о которых следует добавлять в Syslog.
4. Нажмите на кнопку **Сохранить**.

Сведения об ошибках в работе компонентов Kaspersky Private Security Network будут добавляться в Syslog с тегом *KPSN*.

Типы и формат оповещений об ошибках в работе компонентов Kaspersky Private Security Network, добавляемых в Syslog:

- `<Дата и время> <Имя сервера> KPSN[<Идентификатор процесса>]: <Имя процесса> is not available` – указанный процесс недоступен.
- `<Дата и время> <Имя сервера> KPSN[<Идентификатор процесса>]: Server <Имя сервера> is not available` – указанный сервер недоступен.
- `<Дата и время> <Имя сервера> KPSN[<Идентификатор процесса>]: Process <Имя процесса> has problem on server <Имя сервера>` – в работе указанного процесса на указанном сервере обнаружены ошибки.
- `<Дата и время> <Имя сервера> KPSN[<Идентификатор процесса>]: No data in dataflow <Имя потока данных> on <Имя сервера> for an extended period of time` – из указанного потока данных на указанном сервере не приходят сведения.
- `<Дата и время> <Имя сервера> KPSN[<Идентификатор процесса>]: Request errors for service <Идентификатор сервиса> on <Имя сервера>` – ошибка запроса к указанному сервису на указанном сервере.

- `<Дата и время> <Имя сервера> KPSN[<Идентификатор процесса>]: Traffic encryption key <Идентификатор ключа> expired` – истек срок действия ключа шифрования трафика.
- `<Дата и время> <Имя сервера> KPSN[<Идентификатор процесса>]: Traffic encryption key <Идентификатор ключа> expires in <Срок>` – срок действия ключа шифрования трафика истекает через указанное количество времени.
- `<Дата и время> <Имя сервера> KPSN[<Идентификатор процесса>]: Update certificate expired` – истек срок действия сертификата обновлений.
- `<Дата и время> <Имя сервера> KPSN[<Идентификатор процесса>]: Certificate expires in <Срок>` – срок действия сертификата обновлений истекает через указанное количество времени.

  В зависимости от операционной системы сервера, сведения об идентификаторе процесса в журнал Syslog могут не добавляться.

Устранение неполадок в работе компонентов Kaspersky Private Security Network

Этот раздел содержит информацию о методах решения возможных неполадок в работе Kaspersky Private Security Network.

Неполадки, связанные с недоступностью Zabbix

► *Чтобы устранить неполадки в работе Zabbix:*

1. Убедитесь, что на сервере с мониторингом запущен процесс zabbix_server.
2. Убедитесь, что на сервере с мониторингом запущена база данных PostgreSQL.
3. Убедитесь, что на сервере с мониторингом запущен Apache.

Неполадки, связанные с ключами шифрования трафика

► *Чтобы устранить неполадки с ключами шифрования трафика:*

1. Загрузите или создайте новый ключ шифрования трафика (см. раздел "Шифрование трафика" на стр. 36).
2. Запросите новый конфигурационный файл (см. раздел "Отправка запроса в "Лабораторию Касперского"" на стр. 39) у специалистов "Лаборатории Касперского".

Неполадки, связанные с сертификатами обновления

► *Чтобы устранить неполадки, связанные с сертификатами обновления,*

запросите новые сертификаты (см. раздел "Шифрование трафика" на стр. 36) у специалистов "Лаборатории Касперского" (в соответствии с лицензией вашей организации).

Неполадки, связанные с доступом по SSH

► *Чтобы устранить неполадки, связанные с доступом к серверу по SSH:*

1. Убедитесь, что на сервере, на котором регистрируется неполадка, запущен SSHD.
2. Убедитесь, что учетная запись пользователя, от имени которого был добавлен сервер, имеет права на подключение по SSH.
3. Убедитесь, что учетная запись пользователя, от имени которого был добавлен сервер, прописан публичный ключ в файле ~/.ssh/authorized_keys.

   Права доступа к файлу authorized_keys должны быть 600, а доступ к папке .ssh – 700.

4. Убедитесь, что для добавления сервера была использована учетная запись пользователя с достаточными привилегиями sudo (см. раздел "Подготовка к установке программы" на стр. 31): то есть были использованы пользователи kpsn_system_administrator или root.

Неполадки, связанные с активностью процессов

► *Чтобы устранить неполадки, связанные с активностью процессов,*

убедитесь, что сервер соответствует аппаратным требованиям (см. раздел "Аппаратные и программные требования" на стр. 15).

Неполадки, связанные с отставанием обновления баз

► *Чтобы устранить неполадки, связанные с отставанием обновления баз:*

1. Убедитесь, что сервер соответствует аппаратным требованиям (см. раздел "Аппаратные и программные требования" на стр. 15).
2. Убедитесь, что не истек срок действия сертификата (см. раздел "Добавление SSL-сертификата" на стр. 38) для связи с Kaspersky Security Network.
3. Убедитесь в доступности серверов обновления "Лаборатории Касперского".

Неполадки, связанные с качеством обработки запросов

► *Чтобы устранить неполадки, связанные с качеством обработки запросов:*

1. Убедитесь, что сервер соответствует аппаратным требованиям (см. раздел "Аппаратные и программные требования" на стр. 15).
2. Убедитесь, что количество продуктов, подключенных к Kaspersky Private Security Network, соответствует конфигурации (см. раздел "Отправка запроса в "Лабораторию Касперского"" на стр. 39).
3. Убедитесь, что к Kaspersky Private Security Network подключены продукты поддерживаемых версий.

Проверки не проводятся

► *Если вы получаете сообщения, что проверки работоспособности компонентов Kaspersky Private Security Network давно не проводились,*

убедитесь, что на сервере, на котором развернут мониторинг, включена база данных PostgreSQL.

Если вам не удалось самостоятельно устранить неполадку, рекомендуется обратиться в Службу технической поддержки (см. стр. 97).

kaspersky

Управление учетными записями администраторов

Этот раздел содержит информацию об управлении учетными записями администраторов Kaspersky Private Security Network.

В этом разделе

Добавление учетной записи администратора

► *Чтобы добавить учетную запись администратора Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Пользователи**.
3. В панели управления нажмите на кнопку **Добавить**.

   Откроется окно **Добавление нового пользователя**.
4. В поле **Имя пользователя** введите имя новой учетной записи администратора Kaspersky Private Security Network.
5. В полях **Пароль** и **Подтвердите пароль** введите пароль новой учетной записи администратора Kaspersky Private Security Network.
6. Нажмите на кнопку **Добавить**.

Удаление учетных записей администраторов Kaspersky Private Security Network не предусмотрено. Вы можете заблокировать учетную запись администратора Kaspersky Private Security Network, если доступ к веб-интерфейсу Kaspersky Private Security Network под этой учетной записью больше не нужен (см. раздел "Блокирование и разблокирование учетной записи администратора" на стр. 72).

kaspersky

Блокирование и разблокирование учетной записи администратора

► *Чтобы заблокировать или разблокировать учетную запись администратора Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Пользователи**.
3. В столбце **Статус** напротив учетной записи, которую вы хотите заблокировать или разблокировать, выберите значение **Включен** или **Выключен**.

Значение параметра будет применено после следующей авторизации администратора Kaspersky Private Security Network.

Настройка разрешений

Учетная запись администратора (kpsn_admin), созданная при установке Kaspersky Private Security Network, имеет все разрешения. Изменить разрешения для администратора невозможно.

По умолчанию все учетные записи администраторов имеют права на просмотр раздела **Мониторинг**. Если вы хотите запретить просмотр мониторинга для учетной записи администратора, вам потребуется заблокировать эту учетную запись.

► *Чтобы настроить разрешения для учетной записи администратора Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Пользователи**.
3. В списке учетных записей выберите учетную запись администратора Kaspersky Private Security Network, для которого вы хотите настроить разрешения.

   Откроется окно настройки разрешений учетной записи администратора.

4. В блоке **Разрешения** выберите доступные действия в веб-интерфейсе Kaspersky Private Security Network для администратора:

   - **Управление серверами (SC)** – управление серверами с компонентами Kaspersky Private Security Network (добавление и удаление серверов, установка и удаление компонентов).
   - **Управление локальной репутационной базой файлов (FLB)** – добавление или изменение сведений о репутации файлов в базах "Лаборатории Касперского".
   - **Управление локальной репутационной базой веб-сайтов (ULB)** – добавление или изменение сведений о репутации веб-сайтов в базах "Лаборатории Касперского".
   - **Управление учетными записями (AC)** – добавление, блокирование, разблокирование учетных записей администраторов Kaspersky Private Security Network, а также настройка разрешений.
   - **API** – работа с программным интерфейсом Kaspersky Private Security Network (только в режиме HTTPS (см. раздел "Настройка HTTPS" на стр. 41)).

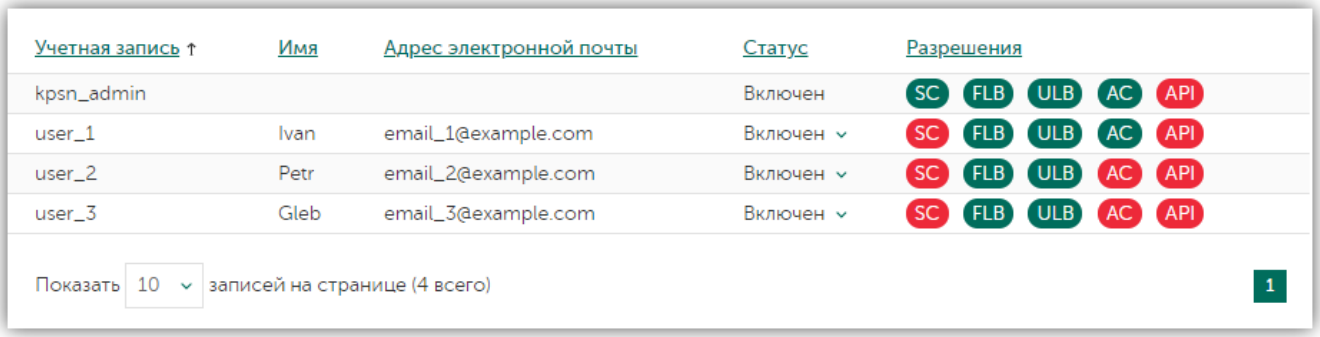


Рисунок 24. Разрешения пользователей

Настройка надежности пароля учетной записи

Вы можете настроить требования к надежности пароля для учетных записей пользователей с помощью *политики паролей*. С помощью политики паролей вы можете задать следующие ограничения использования пароля:

- **Длина пароля**. Максимальное и минимальное количество символов, которые должен содержать пароль.
- **Сложность пароля**. Обязательное использование строчных и прописных букв, специальных символов.
- **История паролей**. Период времени в днях, в течение которого Kaspersky Private Security Network при смене пароля сравнивает новый пароль с использованными ранее. Если пароли совпадают, новый пароль не будет принят. Например, если выбрано значение 90, новый пароль не может совпадать ни с одним из паролей, которые были использованы за последние 90 дней. Если выбрано значение 0, при смене пароля Kaspersky Private Security Network не сравнивает новый пароль с паролями, использованными ранее.
- **Срок действия пароля**. Период времени в днях, в течение которого будет действовать пароль. По истечении установленного срока действия Kaspersky Private Security Network предложит сменить пароль.

Ниже перечислены рекомендованные и используемые по умолчанию требования к надежности пароля для учетных записей пользователей:

- Минимальная длина пароля – 16 символов.
- В пароле должны быть использованы строчные и прописные буквы, а также специальные символы.
- Срок действия пароля – 30 дней.
- Пароли нельзя переиспользовать в течение 90 дней с момента их изменения.

► *Чтобы настроить политику паролей для доступа к Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Пользователи**.
3. В панели управления нажмите на кнопку **Политика пользователей**.

   Откроется окно **Политика паролей**.
4. Настройте параметры политики паролей.

В Kaspersky Private Security Network действует новая политика паролей для доступа к приложению.

При изменении одного или нескольких указанных ниже требований к надежности паролей всем пользователям Kaspersky Private Security Network потребуется задать новые пароли при следующем входе в приложение или выполнении любого действия в веб-интерфейсе приложения, даже если текущие пароли отвечают новым требованиям:

- Новая минимальная длина пароля больше старой минимальной длины пароля.
- Новая максимальная длина пароля меньше старой максимальной длины пароля.
- Включено требование иметь в пароле латинские символы в нижнем регистре.
- Включено требование иметь в пароле латинские символы в верхнем регистре.
- Включено требование иметь в пароле специальные символы.

kaspersky

Изменение пароля учетной записи администратора

Изменение пароля учетной записи администратора Kaspersky Private Security Network может быть выполнено следующими способами:

- при входе в веб-интерфейс Kaspersky Private Security Network во время авторизации;
- во время работы в веб-интерфейсе Kaspersky Private Security Network.

► *Чтобы изменить пароль учетной записи администратора Kaspersky Private Security Network во время работы в веб-интерфейсе Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Нажмите на ссылку с именем пользователя в правом верхнем углу веб-интерфейса.
3. В выпадающем меню выберите **Изменить пароль**.
4. Введите текущий пароль учетной записи администратора, созданной при установке Kaspersky Private Security Network, в поле **Текущий пароль**.
5. В полях **Новый пароль** и **Подтвердите пароль** введите новый пароль учетной записи администратора Kaspersky Private Security Network.
6. Нажмите на кнопку **Сохранить изменения**.

Значение параметра будет применено после следующей авторизации администратора Kaspersky Private Security Network.

kaspersky

Работа с API

Программный интерфейс Kaspersky Private Security Network (далее также "API") – набор REST-компонентов, позволяющий отправлять запросы в Kaspersky Private Security Network с любого компьютера локальной сети организации без использования браузера. API позволяет выделить отдельного пользователя для администрирования локальных репутационных баз. При этом веб-интерфейс Kaspersky Private Security Network пользователю не требуется. Для администрирования баз пользователь должен получить разрешения на управление локальными репутационными базами (см. раздел "Настройка разрешений" на стр. 72).

Работа с API осуществляется только по протоколу HTTPS (см. раздел "Настройка HTTPS" на стр. 41).

С помощью API вы можете выполнять следующие действия:

- добавлять сведения о репутации файлов или веб-сайтов в локальные репутационные базы;
- удалять сведения о репутации файлов или веб-сайтов из локальной репутационной базы;
- проверять репутацию отдельных файлов или веб-сайтов.

Перед отправкой запроса необходимо пройти аутентификацию на серверах с установленными компонентами File Reputation и URL Reputation (см. раздел "Аутентификация на основе сертификатов" на стр. 78). Взаимодействие с серверами осуществляется по протоколу HTTPS.

Размер запроса не должен превышать 128 КБ. Если размер запроса превышает 128 КБ, запрос не будет обработан, отобразится ошибка `413 Request Entity Too Large`.

Для отправки запросов на компьютере должен быть установлен REST-клиент (например, Insomnia, см. рис. ниже). Вы также можете отправлять запросы с помощью интерпретатора командной строки (например, cURL).

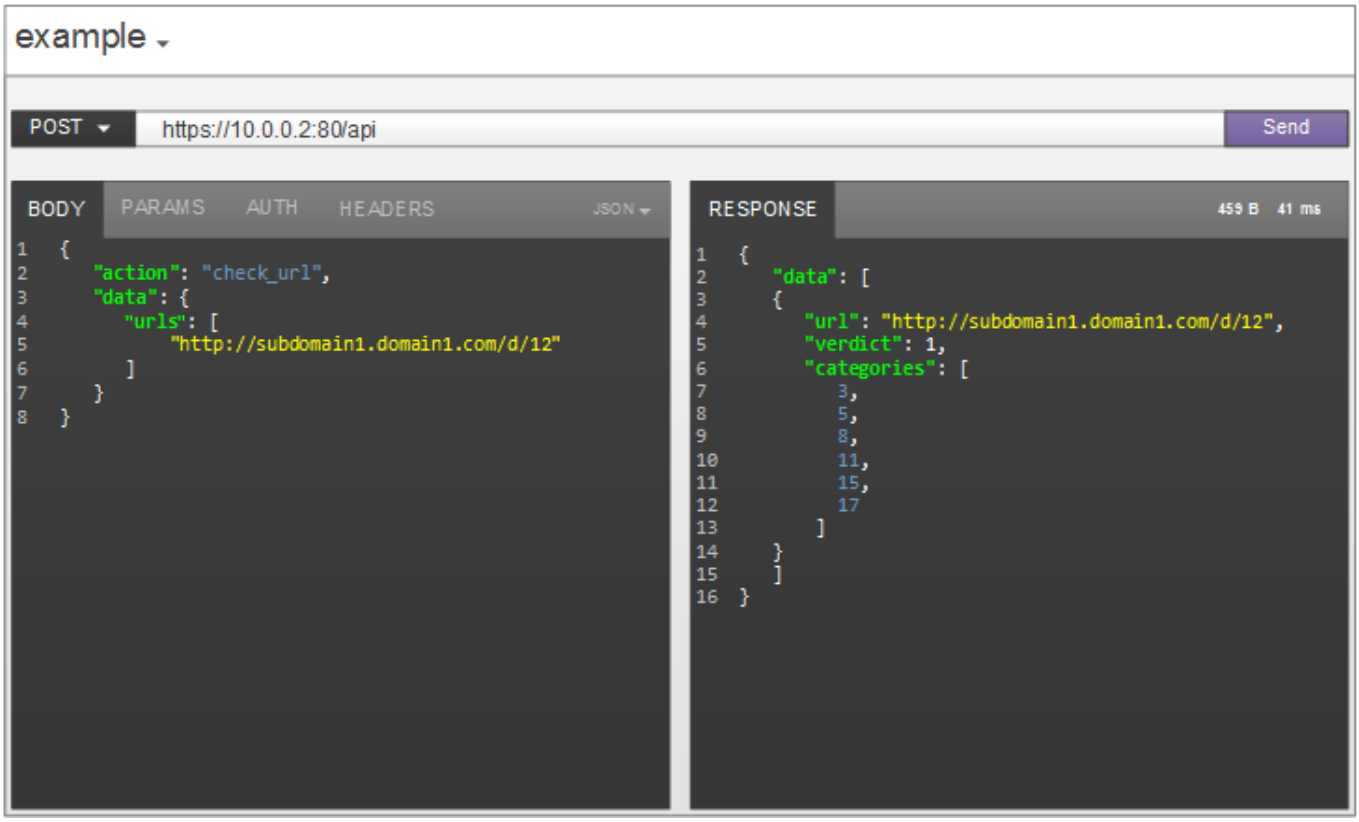


Рисунок 25. Окно REST-клиента с примером запроса репутации веб-сайтов

В этом разделе

kaspersky

Аутентификация на основе сертификатов

Для отправки запросов в Kaspersky Private Security Network с помощью API необходимо выполнить аутентификацию пользователя в Kaspersky Private Security Network. Аутентификация пользователя выполняется на основе сертификата и ключа для API.

Перед аутентификацией пользователя необходимо выполнить следующие действия:

1. Получить сертификат и ключ для API в веб-интерфейсе Kaspersky Private Security Network.
2. Добавить сертификат и ключ для API на компьютер, с которого пользователь будет выполнять запросы.
3. Добавить сертификат и ключ для API в параметрах аутентификации REST-клиента или выполнить команду аутентификации в Kaspersky Private Security Network.

► *Чтобы получить сертификат и ключ для API:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Нажмите на ссылку с именем пользователя в правом верхнем углу веб-интерфейса.
3. В выпадающем меню выберите **Мой профиль**.

   Откроется окно с информацией о пользователе.
4. Нажмите на кнопку **Сертификат клиента**.

Kaspersky Private Security Network загрузит ZIP-архив с сертификатом и ключом для API в директорию для загрузки по умолчанию.

Затем вам нужно перенести ZIP-архив на компьютер, с которого пользователь будет выполнять запросы. Далее добавьте сертификат и ключ для API в параметрах аутентификации REST-клиента или выполните команду в интерпретаторе командной строки (например, cURL).

Пример команды аутентификации

```
curl --cert <certificate> --key <key> -X POST -d <data>
https://<server>:80/api/
Здесь:
<certificate> – путь к сертификату.
<key> – путь к ключу.
<data> – запрос.
<server> – IP-адрес сервера с установленным компонентом Monitoring
System.
```

kaspersky

Добавление сведений о репутации файла

Запрос

Запрос на добавление сведений о репутации файла содержит следующие параметры:

- `action` – запрос на выполнение действия с Kaspersky Private Security Network (значение `add_file`).
- `data.hash_type` – алгоритм хеширования. Возможные значения:
  - `sha256`;
  - `md5`.

  > В одном запросе вы можете указать только один алгоритм хеширования (например, только SHA256). Если хеш файла не соответствует значению `data.hash_type`, запрос не будет обработан, отобразится ошибка `203 hash type mismatch`.

- `data.force` – устранение конфликтов добавления репутации файла (необязательный параметр). Kaspersky Private Security Network проверяет наличие добавленных ранее сведений о репутации файла в локальной репутационной базе и сведений в базе Kaspersky Security Network (KL-репутация). Возможные значения:
  - `true` – изменение текущей репутации на репутацию в запросе в любом случае.
  - `false` – изменение текущей репутации на репутацию в запросе, только если в Kaspersky Private Security Network нет сведений о репутации файла. Если в Kaspersky Private Security Network уже добавлены сведения о файле, репутация не будет изменена. Значение по умолчанию.
- `data.hashes` (массив):
  - `data.hashes.hash` – хеш файла: MD5 (строка 16 байт) или SHA256 (строка 32 байта).
  - `data.hashes.reputation` – репутация файла. Возможные значения:
    - `1` – доверенный;
    - `2` – недоверенный.
  - `data.hashes.file_name` – имя файла (строка до 256 символов).
  - `data.hashes.description` – дополнительное описание файла (строка до 1024 символов).

► *Чтобы добавить сведения о репутации файла:*

1. Запустите REST-клиент на любом компьютере локальной сети организации, имеющем доступ к серверу Monitoring System.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите IP-адрес сервера с компонентом Monitoring System:

   `https://<IP-адрес сервера с компонентом Monitoring System>:80/api`
4. В рабочей области введите содержание запроса в формате JSON. См. пример запроса ниже.
5. Отправьте запрос сервису File Reputation.

   В окне REST-клиента отобразится ответ с результатом выполнения запроса.

Пример запроса

```
{
    "action": "add_file",
    "data": {
        "hash_type": "sha256",
        "force": false,
        "hashes": [
        {
            "hash":
"9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203",
            "reputation": 1,
            "file_name": "file1.exe",
            "description": "trust file, sha256 hash"
        },
        {
            "hash":
"9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307204",
            "reputation": 2,
            "file_name": "file2.exe",
            "description": "untrust file, sha256 hash"
        }
        ]
    }
}
```

Ответ

Ответ содержит следующую информацию:

- `data.hash` – хеш файла (массив): MD5 (строка 16 байт) или SHA256 (строка 32 байта).
- `data.publish_status` – результат выполнения запроса. Возможные значения:
  - `true` – сведения о файле успешно добавлены в локальную репутационную базу.
  - `false` – добавить сведения о файле в локальную репутационную базу не удалось. В локальной репутационной базе уже содержатся сведения о файле. Чтобы изменить сведения о файле, необходимо установить для параметра `data.force` значение `true`.

Пример ответа

```
{
    "data": [
        {
            "hash":
"9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203",
            "publish_status": true
        },
        {
            "hash":
"9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307204",
            "publish_status": false
        }
    ]
}
```

Добавление сведений о репутации веб-сайта

Запрос

Запрос на добавление сведений о репутации веб-сайта содержит следующие параметры:

- `action` – запрос на выполнение действия с Kaspersky Private Security Network (значение `add_url`).
- `data.force` – устранение конфликтов добавления репутации веб-сайта (необязательный параметр). Kaspersky Private Security Network проверяет наличие добавленных ранее сведений о репутации веб-сайта в локальной репутационной базе и сведений в базе Kaspersky Security Network (KL-репутация). Возможные значения:
  - `true` – изменение текущей репутации на репутацию в запросе в любом случае.
  - `false` – изменение текущей репутации на репутацию в запросе, только если в Kaspersky Private Security Network нет сведений о репутации веб-сайта. Если в Kaspersky Private Security Network уже добавлены сведения о веб-сайте, репутация не будет изменена. Значение по умолчанию.
- `data.urls` (массив):
  - `data.urls.url` – URL-адрес веб-сайта. URL-адрес должен удовлетворять требованию RFC 3986, допускается использование маски (*).
  - `data.urls.reputation` – репутация веб-сайта. Возможные значения:
    - `1` – доверенный;
    - `2` – недоверенный.
  - `data.urls.description` – дополнительное описание веб-сайта (строка до 1024 символов).

► *Чтобы добавить сведения о репутации веб-сайта:*

1. Запустите REST-клиент на любом компьютере локальной сети организации, имеющем доступ к серверу Monitoring System.
2. В списке методов выберите метод POST.

3. В поле адреса запроса введите IP-адрес сервера с компонентом Monitoring System:

   `https://<IP-адрес сервера с компонентом Monitoring System>:80/api`

4. В рабочей области введите содержание запроса в формате JSON. См. пример запроса ниже.
5. Отправьте запрос сервису URL Reputation.

   В окне REST-клиента отобразится ответ с результатом выполнения запроса.

Пример запроса

```
{
    "action": "add_url",
    "data": {
        "force": false,
        "urls": [
        {
            "url": "website1.com",
            "reputation": 1,
            "description": "social network"
        },
        {
            "url": "website2.com",
            "reputation": 2,
            "description": "network game"
        }
        ]
    }
}
```

Ответ

Ответ содержит следующую информацию:

- `data.url` – URL-адрес веб-сайта (массив).
- `data.publish_status` – результат выполнения запроса. Возможные значения:
  - `true` – сведения о веб-сайте успешно добавлены в локальную репутационную базу.
  - `false` – добавить сведения о веб-сайте в локальную репутационную базу не удалось. В локальной репутационной базе уже содержатся сведения о веб-сайте. Чтобы изменить сведения о веб-сайте, необходимо установить для параметра `data.force` значение `true`.

Пример ответа

```
{
    "data": [
    {
        "url": "website1.com",
        "publish_status": true
    },
    {
        "url": "website2.com",
        "publish_status": false
    }
    ]
}
```

Удаление сведений о репутации файла

Запрос

Запрос на удаление сведений о репутации файла содержит следующие параметры:

- `action` – запрос на выполнение действия с Kaspersky Private Security Network (значение `delete_file`).
- `data.hash_type` – алгоритм хеширования. Возможные значения:
  - `sha256`;
  - `md5`.

  > В одном запросе вы можете указать только один алгоритм хеширования (например, только SHA256). Если хеш файла не соответствует значению `data.hash_type`, запрос не будет обработан, отобразится ошибка `203 hash type mismatch`.

- `data.hashes` – хеш файлов (массив): MD5 (строка 16 байт) или SHA256 (строка 32 байта).

► *Чтобы удалить сведения о репутации файла:*

1. Запустите REST-клиент на любом компьютере локальной сети организации, имеющем доступ к серверу Monitoring System.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите IP-адрес сервера с компонентом Monitoring System:

   `https://<IP-адрес сервера с компонентом Monitoring System>:80/api`
4. В рабочей области введите содержание запроса в формате JSON. См. пример запроса ниже.
5. Отправьте запрос сервису File Reputation.

   В окне REST-клиента отобразится ответ с результатом выполнения запроса.

Пример запроса

```
{
    "action": "delete_file",
    "data": {
        "hash_type": "sha256",
        "hashes": [

"9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203"
        ]
    }
}
```

Ответ

Ответ содержит хеш удаленных файлов, а также код и описание ошибки, если запрос выполнить не удалось.

Пример ответа

```
{
    "data": [
        {
            "hash":
"9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203"
        }
    ]
}
```

Удаление сведений о репутации веб-сайта

Запрос

Запрос на удаление сведений о репутации веб-сайта содержит следующие параметры:

- `action` – запрос на выполнение действия с Kaspersky Private Security Network (значение `delete_url`).
- `data.urls` – URL-адреса веб-сайтов (массив). URL-адреса должны удовлетворять требованию RFC 3986.

► *Чтобы удалить сведения о репутации веб-сайта:*

1. Запустите REST-клиент на любом компьютере локальной сети организации, имеющем доступ к серверу Monitoring System.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите IP-адрес сервера с компонентом Monitoring System:

   `https://<IP-адрес сервера с компонентом Monitoring System>:80/api`
4. В рабочей области введите содержание запроса в формате JSON. См. пример запроса ниже.
5. Отправьте запрос сервису URL Reputation.
6. В окне REST-клиента отобразится ответ с результатом выполнения запроса.

Пример запроса

```
{
    "action": "delete_url",
    "data": {
        "urls": [
            "website1.com"
        ]
    }
}
```

Ответ

Ответ содержит URL-адреса удаленных веб-сайтов, а также код и описание ошибки, если запрос выполнить не удалось.

Пример ответа

```
{
    "data": [
        {
            "url": "website1.com"
        }
    ]
}
```

Проверка репутации файлов

Запрос

Запрос проверки репутации файла содержит следующие параметры:

- `action` – запрос на выполнение действия с Kaspersky Private Security Network (значение `check_file`).
- `data.hash_type` – алгоритм хеширования. Возможные значения:
  - `sha256`;
  - `md5`.

  > В одном запросе вы можете указать только один алгоритм хеширования (например, только SHA256). Если хеш файла не соответствует значению `data.hash_type`, запрос не будет обработан, отобразится ошибка `203 hash type mismatch`.

- `data.hashes` – хеш файлов (массив): MD5 (строка 16 байт) или SHA256 (строка 32 байта).

► *Чтобы проверить репутацию файла:*

1. Запустите REST-клиент на любом компьютере локальной сети организации, имеющем доступ к серверу Monitoring System.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите IP-адрес сервера с компонентом Monitoring System:

```
https://<IP-адрес сервера с компонентом Monitoring System>:80/api
```

4. В рабочей области введите содержание запроса в формате JSON. См. пример запроса ниже.
5. Отправьте запрос сервису File Reputation.

   В окне REST-клиента отобразится ответ с результатом выполнения запроса.

Пример запроса

```
{
    "action": "check_file",
    "data": {
        "hash_type": "sha256",
        "hashes": [

"9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203"
        ]
    }
}
```

Ответ

На основе ответа о репутации файла вы можете оценить безопасность использования этого файла. Ответ содержит следующую информацию:

Параметр	Описание	Всегда есть в ответе
`hash`	Хеш файла (массив): MD5 (строка 16 байт) или SHA256 (строка 32 байта).	Да
`reputation`	Репутация файла. Возможные значения: • `0` – неизвестный; • `1` – доверенный; • `2` – недоверенный; • `-1` – неопределенный.	Да
`description`	Дополнительные сведения о репутации файла.	Нет
`product`	Название программы, которой принадлежит файл.	Нет
`vendor`	Название издателя файла.	Нет
`users`	Количество пользователей Kaspersky Security Network, использующих этот файл (только для доверенных файлов)	Нет
`firstRequest`	Дата и время, когда файл стал известен в Kaspersky Security Network.	Нет
`groupSharing`	Процентное распределение файла по группам доверия программ "Лаборатории Касперского", отправляющих данные в Kaspersky Security Network. Группы доверия: • `trusted` – доверенный; • `untrusted` – недоверенный;	Нет

Параметр	Описание	Всегда есть в ответе
	• `low` – сильные ограничения; • `high` – слабые ограничения.	
`geoSharing`	Процентное распределение обнаружений файла по странам. Страны указываются в виде двухбуквенного кода. `00` означает сведенную в одну категорию статистику по нескольким странам.	Нет
`client_data`	Идентификатор источника информации в ответе: • `true` – репутация из источников вашей организации; • `false` – репутация из баз Kaspersky Private Security Network.	Да

Пример ответа:


```
{
    "data": [
        {
            "hash":
"9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203",
            "reputation": 2,
            "firstRequest": "1601-00-01T00:00:01Z",
            "users": 123,
            "product": "program",
            "vendor": "company",
            "client_data": "true",
            "groupSharing": {
                "high": 30,
                "low": 20,
                "trusted": 10,
                "untrusted": 40
            },
            "geoSharing": {
                "fr": 25,
                "it": 19,
                "uk": 15,
                "es": 12,
                "mx": 10,
                "00": 17
            }
        }
    ]
}
```

kaspersky

Проверка репутации веб-сайтов

Запрос

Запрос проверки репутации веб-сайта содержит следующие параметры:

- `action` – запрос на выполнение действия с Kaspersky Private Security Network (значение `check_url`).
- `data.urls` – URL-адреса веб-сайтов (массив). URL-адреса должны удовлетворять требованию RFC 3986.

► *Чтобы проверить репутацию веб-сайта:*

1. Запустите REST-клиент на любом компьютере локальной сети организации, имеющем доступ к серверу Monitoring System.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите IP-адрес сервера с компонентом Monitoring System:

   `https://<IP-адрес сервера с компонентом Monitoring System>:80/api`
4. В рабочей области введите содержание запроса в формате JSON. См. пример запроса ниже.
5. Отправьте запрос сервису URL Reputation.

   В окне REST-клиента отобразится ответ с результатом выполнения запроса.

Пример запроса:

```
{
    "action": "check_url",
    "data": {
        "urls": [
            "website1.com"
        ]
    }
}
```

Ответ

На основе ответа о репутации веб-сайта вы можете оценить безопасность посещения этого веб-сайта. Ответ содержит следующую информацию:

Параметр	Описание	Всегда есть в ответе
`url`	URL-адрес веб-сайта (массив).	Да
`reputation`	Репутация веб-сайта. Возможные значения: • `0` – неизвестный; • `1` – доверенный; • `2` – недоверенный;	Да

Параметр	Описание	Всегда есть в ответе
	• `-1` – неопределенный.	
`ttl`	Рекомендуемое время (в секундах), на которое клиент может закешировать полученный ответ	Да
`categories`	Список с идентификаторами категорий веб-сайта (см. раздел "Список категорий веб-сайтов сервиса URL Reputation" на стр. 102). Если информация по запрошенному веб-адресу отсутствует, выводится пустой список.	Да
`client_data`	Идентификатор источника информации в ответе: • `true` – репутация из источников вашей организации; • `false` – репутация из баз Kaspersky Private Security Network.	Да

Пример ответа:

```
{
    "data": [
    {
        "url": "website1.com",
         "reputation": 1,
         "categories": [
             3,
             5,
             8
         ],
         "ttl": 3600,
         "client_data": "true"
    }
    ]
}
```

kaspersky

Коды ошибок

Во время работы с API возможны сбои в работе Kaspersky Private Security Network. Каждой ошибке присвоен код (см. таблицу ниже).

Таблица 3. Коды ошибок

Код ошибки	Описание (категория ошибки)	Рекомендации
1	Пропущен необходимый параметр (общее).	Проверьте правильность ввода запроса. Убедитесь, что в запросе перечислены все необходимые параметры и параметры указаны верно.
2	Недопустимый тип параметра (общее).	Проверьте правильность ввода запроса. Убедитесь, что все значения параметров указаны верно.
3	Синтаксическая ошибка в запросе (общее).	Проверьте правильность ввода запроса. Например, для параметра `action` может быть указано значение `check url`, а не `checl_url`.
4	Недопустимый код JSON (общее).	Проверьте правильность ввода запроса. Подробнее о формате JSON см. в справочнике по скриптам JSON ADF.
5	Повторяющийся запрос (общее).	Проверьте правильность ввода запроса. Возможно, вы уже отправляли этот запрос ранее.
51	У пользователя нет разрешения для работы с API (аутентификация).	Предоставьте пользователю разрешение для работы с API (см. раздел "Настройка разрешений" на стр. 72).
52	Учетная запись пользователя заблокирована (аутентификация).	Разблокируйте учетную запись пользователя (см. раздел "Блокирование и разблокирование учетной записи администратора" на стр. 72).
53	Неправильные учетные данные (аутентификация).	Получите сертификат и ключ для API в веб-интерфейсе Kaspersky Private Security Network еще раз и повторите аутентификацию (см. раздел "Аутентификация на основе сертификатов" на стр. 78).
101	Неизвестная репутация объекта (локальная репутационная база).	Убедитесь, что значение параметра репутации объекта (`reputation`) указано верно. Возможные значения: • `1` – доверенный; • `2` – недоверенный.
151	Короткий URL-адрес (URL Reputation).	Убедитесь, что URL-адрес соответствует RFC 3986. Введите URL-адрес по шаблону `example.com`
152	Недопустимый URL-адрес веб-сайта (URL Reputation).	Убедитесь, что URL-адрес соответствует RFC 3986. Регулярные выражения в URL-адресе не допускаются.

Код ошибки	Описание (категория ошибки)	Рекомендации
153	URL-адрес не удалось обработать (URL Reputation).	Убедитесь, что URL-адрес соответствует RFC 3986. Введите URL-адрес по шаблону example.com
201	Недопустимый хеш файла (File Reputation).	Убедитесь, что хеш файла введен корректно. Kaspersky Private Security Network поддерживает работу с алгоритмами хеширования MD5 и SHA256.
202	Хеш файла пустой (File Reputation).	Введение хеш файла (hash). Kaspersky Private Security Network поддерживает работу с алгоритмами хеширования MD5 и SHA256.
203	Хеш файла не соответствует заявленному алгоритму хеширования (File Reputation).	Убедитесь, что параметр алгоритма хеширования (hash_type) указан верно.
204	Неизвестный алгоритм хеширования (File Reputation).	Убедитесь, что для параметра алгоритма хеширования (hash_type) указано значение MD5 и SHA256. Kaspersky Private Security Network не поддерживает другие алгоритмы хеширования.
255	Неизвестная ошибка (общее).	Обратитесь в Службу технической поддержки.

kaspersky

Журнал Kaspersky Private Security Network

Журнал Kaspersky Private Security Network предназначен для диагностики и решения возникших проблем в работе программы. В журнал Kaspersky Private Security Network записывается информация о событиях, которые произошли во время работы Kaspersky Private Security Network.

Kaspersky Private Security Network не передает данные за пределы локальной сети организации, а сохраняет данные внутри локальной сети. Журнал Kaspersky Private Security Network хранится в директории /usr/local/ksn/log/ на каждом сервере Kaspersky Private Security Network. Выключить запись информации в журнал Kaspersky Private Security Network невозможно, за исключением записи в журнал запросов для сервисов Url Reputation и File Reputation.

В журнал Kaspersky Private Security Network записываются следующие данные:

- Системная информация о работе сервисов Kaspersky Private Security Network (например, статусы серверов, статусы сервисов, информация о последнем обновлении).
- IP-адреса компьютеров пользователей программ "Лаборатории Касперского", с которых выполнялся запрос к Kaspersky Private Security Network.
- Информация о работе Файлового Антивируса:
  - Хеш проверяемых файлов;
  - Хеш сертификатов проверяемых файлов.
- Информация о сетевой активности пользователей:
  - URL-адреса посещаемых веб-сайтов.
  - IP-адреса посещаемых ресурсов.
  - Имена посещаемых хостов.

  > Учетные данные пользователей (имя пользователя и пароль) в журнал Kaspersky Private Security Network не записываются.

- Информация о входящей электронной почте:
  - IP-адреса отправителей сообщений электронной почты.
  - Хеш файлов во вложении сообщений электронной почты.
  - URL-адреса, содержащиеся в сообщениях электронной почты.
- Системная информация о работе программ "Лаборатории Касперского":
  - Идентификатор компьютера, на котором установлена программа "Лаборатории Касперского".
  - Идентификатор пользователя программы "Лаборатории Касперского".
  - Названия обнаруженных угроз.
- Запросы для сервисов URL Reputation и File Reputation.

Запись запросов для сервисов URL Reputation и File Reputation можно включить или выключить. (см. раздел "Включение и выключение записи запросов для сервисов URL Reputation и File Reputation" на стр. 93)

Файлы журналов Kaspersky Private Security Network автоматически архивируются для экономии дискового пространства на серверах. Архивы журнала Kaspersky Private Security Network хранятся на сервере 10 дней. По истечении 10 дней архивы удаляются.

Архивы журнала имеют ограничение на размер в 10 ГБ. Когда этот размер достигнут, при добавлении в архив новых записей более ранние записи удаляются.

Вы также можете настроить ротацию файлов журнала Kaspersky Private Security Network на каждом сервере Kaspersky Private Security Network с помощью утилиты logrotate, входящей в состав операционной системы. Подробнее о работе утилиты logrotate см. в документации к операционной системе.

В этом разделе

kaspersky

Включение и выключение записи запросов для сервисов URL Reputation и File Reputation

Запись запросов для сервисов URL Reputation и File Reputation можно включить или выключить. Когда запись в журнал запросов на сервере, с которого идет запись, включена, отображается зеленый значок **LOGS**. Если запись запросов на сервере выключена, отображается красный значок **LOGS**.

Если сервисы URL Reputation и File Reputation установлены на одном сервере, запись запросов включается или выключается сразу для обоих сервисов.

► *Чтобы включить запись в журнал запросов для сервисов URL Reputation и File Reputation:*

1. Откройте веб-интерфейс Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. Выберите сервер, на котором вы хотите включить логирование запросов URL Reputation и File Reputation.
4. Нажмите на кнопку **Включить логирование запросов**.

Запросы для сервисов URL Reputation и File Reputation будут записываться в журнал Kaspersky Private Security Network.

► *Чтобы выключить запись в журнал запросов для сервисов URL Reputation и File Reputation:*

1. Повторите пункты 1–2 из инструкции выше.
2. Выберите сервер, на котором вы хотите выключить логирование запросов URL Reputation и File Reputation.
3. Нажмите на кнопку **Выключить логирование запросов**.

Запросы для сервисов URL Reputation и File Reputation перестанут записываться в журнал Kaspersky Private Security Network.

Управление программой через Kaspersky Security Center

Kaspersky Security Center – программа для централизованного дистанционного управления и обслуживания системы защиты организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, основанной на использовании программ "Лаборатории Касперского".

При работе с Kaspersky Security Center вы можете настроить использование в локальной сети организации Kaspersky Private Security Network вместо Kaspersky Security Network.

Для использования Kaspersky Private Security Network на компьютере администратора должен быть установлен Kaspersky Security Center версии 10 Service Pack 1 или выше.

► *Чтобы использовать Kaspersky Private Security Network в Kaspersky Security Center,*

загрузите конфигурационный файл, полученный после отправки запроса в "Лабораторию Касперского" (см. раздел "Добавление ключа шифрования трафика" на стр. 36), в окне свойств Сервера администрирования. Подробную информацию о настройке Kaspersky Private Security Network в Kaspersky Security Center см. в *Руководстве администратора Kaspersky Security Center*.

Пользователи компьютеров, на которые установлены программы "Лаборатории Касперского", получат доступ к репутационным базам Kaspersky Private Security Network.

kaspersky

Устранение сбоев передачи данных через однонаправленный шлюз

Во время загрузки пакетов с репутационными базами из открытого сегмента сети в категорированный сегмент сети через однонаправленный шлюз может произойти сбой. Об ошибке вы можете узнать в веб-интерфейсе категорированного сегмента сети Kaspersky Private Security Network. При возникновении ошибки в веб-интерфейсе категорированного сегмента сети в окне **Статус серверов** рядом с IP-адресом сервера с компонентом Gateway Output отображается значок .

► *Чтобы устранить ошибку загрузки обновлений баз:*

1. Откройте веб-интерфейс категорированного сегмента сети Kaspersky Private Security Network в окне браузера (см. раздел "Вход в веб-интерфейс Kaspersky Private Security Network" на стр. 34).
2. Выберите раздел **Серверы**.
3. Нажмите на значок рядом с IP-адресом сервера с установленным компонентом Gateway Output.

   Откроется окно **Статус потоков данных** с потоками данных, во время загрузки которых произошла ошибка, выделенными красным цветом.
4. Запишите или сохраните имена потоков данных, выделенных красным цветом, и коды их статусов.
5. Откройте веб-интерфейс открытого сегмента сети Kaspersky Private Security Network в окне браузера.
6. Выберите раздел **Серверы**.
7. Нажмите на значок рядом с IP-адресом сервера с установленным компонентом Gateway Input.

   Откроется окно **Обновление потока данных**.
8. Выберите сервис, при загрузке данных которого произошла ошибка.
9. В поле справа от выбранного потока обновлений введите код доступа этого потока обновлений, записанный вами при работе с веб-интерфейсом категорированного сегмента сети.
10. Нажмите на кнопку **Обновить**.

    Поток обновлений будет загружен на сервер категорированного сегмента сети.

В списке серверов раздела **Серверы** окна **Статус серверов** веб-интерфейса категорированного сегмента сети рядом с IP-адресом сервера с компонентом Gateway Output отобразится значок .

kaspersky

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в источниках информации о программе (см. раздел "Источники информации о программе" на стр. 10), рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского". Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Kaspersky предоставляет поддержку этой программы в течение ее жизненного цикла https://support.kaspersky.com/corporate/lifecycle.
Прежде чем обратиться в Службу технической поддержки, рекомендуется ознакомиться с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки "Лаборатории Касперского" по телефону;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" через портал Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

kaspersky

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

В этом разделе

kaspersky

Список портов для работы программы

Ниже перечислены порты, которые требуется открыть для работы Kaspersky Private Security Network.

Порты, которые необходимо открыть во всех комплектациях Kaspersky Private Security Network

Инициатор соединения	Цель соединения	Порт	Протокол	Описание
Сервер мониторинга	Сервер KPSN	22	SSH	Управление серверами KPSN
Сервер мониторинга	Сервер KPSN	161	UDP	Получение метрик
Сервер мониторинга	Сервер KPSN	2812	HTTP	Получение статуса сервера
Сервер мониторинга	Сервер мониторинга	8008	HTTP	Доступ в систему агрегации счетчиков
Сервер мониторинга	Сервер мониторинга	5432	TCP	Доступ к локальной БД
Сервер мониторинга	Сервер KPSN с компонентами File Reputation и/или Url Reputation	8080	HTTP	Запрос репутации
Сервер мониторинга	Сервер KPSN с компонентами File Reputation и/или Url Reputation	9009	HTTPS	Публикация пользовательских данных
Сервер KPSN с компонентом KMP	Сервер KPSN с компонентом Additional Services	5671	AMQP	Данные KMP
Продукт Лаборатории Касперского	Сервер KPSN с сервисами	443	TCP	Запрос репутации
Веб-браузер администратора	Сервер мониторинга	80	HTTP/HTTPS	Доступ к веб-интерфейсу KPSN (протокол определяется режимом работы KPSN)
Клиент REST API	Сервер мониторинга	80	HTTPS	Использование api KPSN

Порты, которые необходимо открыть в комплектациях Kaspersky Private Security Network без прокси-сервера и однонаправленного шлюза

Инициатор соединения	Цель соединения	Порт	Протокол	Описание
Сервер KPSN с сервисами	Серверы обновления Лаборатории Касперского	443	HTTPS	Запрос обновлений
Сервер KPSN с сервисами	Сервера обновления Лаборатории Касперского	5671	AMQPS	Получение обновлений

Порты, которые необходимо открыть в комплектациях Kaspersky Private Security Network с прокси-сервером

Инициатор соединения	Цель соединения	Порт	Протокол	Описание
Сервер KPSN с компонентом Proxy	Сервера обновления Лаборатории Касперского	443	HTTPS	Запрос обновлений
Сервер KPSN с компонентом Proxy	Сервера обновления Лаборатории Касперского	5671	AMQPS	Получение обновлений
Сервер KPSN с сервисами	Сервер KPSN с компонентом Proxy	22	SSH	Установка ssh-туннелей для доступа на серверы обновления Лаборатории Касперского

Порты, которые необходимо открыть в комплектациях Kaspersky Private Security Network с однонаправленным шлюзом

Инициатор соединения	Цель соединения	Порт	Протокол	Описание
Сервер KPSN Gateway Input	Серверы обновлений Лаборатории Касперского	443	HTTPS	Запрос обновлений
Сервер KPSN Gateway Input	Серверы обновлений Лаборатории Касперского	5671	AMQPS	Получение обновлений
Сервер KPSN с сервисами	Сервер KPSN Gateway Output	442	HTTPS	Запрос обновлений
Сервер KPSN с сервисами	Сервер KPSN Gateway Output	5671	AMQPS	Получение обновлений

Разрешите исходящее соединение на ksn-pub-3.kaspersky-labs.com (IP-адреса: 62.128.100.*, 77.74.179.*, 77.74.177.*) на порты 443, 5671 и localhost на порт 8008 для следующих серверов:

- Для всех серверов с компонентами программы, если вы используете стандартную комплектацию Kaspersky Private Security Network.
- Для сервера с компонентом Gateway Input, если вы используете Kaspersky Private Security Network с однонаправленным шлюзом.
- Для сервера с компонентом Proxy, если вы используете Kaspersky Private Security Network с прокси-сервером.

Список пакетов, необходимых для работы Kaspersky Private Security Network

На серверах, на которые устанавливаются компоненты Kaspersky Private Security Network, должны быть установлены следующие пакеты:

Системные пакеты:

- acl
- apache2
- curl
- libapache2-mod-wsgi-py3
- libapache2-mod-php
- python3-bcrypt
- python3-cryptography
- python3-dateutil
- python3-defusedxml
- python3-django

- python3-openssl
- python3-paramiko
- python3-psycopg2
- python3-requests
- python3-urllib3
- postgresql
- snmpd
- sudo
- zabbix-server-pgsql
- zabbix-frontend-php

> Подробнее об установке Zabbix см. в документации https://www.zabbix.com/documentation/current/ru/manual/installation/install_from_packages/rhel_centos на официальном сайте решения.

Пакеты pip3:

- flup
- puka
- gevent

Список категорий веб-сайтов сервиса URL Reputation

Проверка репутации веб-сайтов с помощью HTTP-запроса сервисам URL Reputation также включает в себя определение категорий веб-сайтов. Если идентификатор категории веб-сайтов отсутствует в списке, для текущей версии Kaspersky Private Security Network эта категория неизвестна. В документации для следующей версии Kaspersky Private Security Network список категорий будет обновлен. Ниже приведен список идентификаторов и категорий веб-сайтов.

Таблица 4. Категории веб-сайтов сервиса URL Reputation

Идентификатор	Категория веб-сайта
0	Категория не присвоена
1	Для взрослых
2	Запрещенное ПО
3	Алкоголь, табак, наркотики и психотропы
4	Насилие
5	Нецензурная лексика
6	Оружие, взрывчатые вещества, пиротехника
7	Азартные игры

8	Чаты, форумы, IM
9	Веб-почта
10	Интернет-магазины
11	Социальные сети
12	Поиск работы
13	Средства анонимного доступа
14	Платежные системы
15	Казуальные видеоигры
16	Платежные системы
17	Банковские веб-ресурсы
18	Дискриминация
19	Фрондерство
20	Онлайн-магазины с собственной платежной системой
21	Запрещено полицией Японии
22	Программное обеспечение, аудио, видео
23	Финансы, экономика
24	Бизнес
25	Компьютерная техника, электроника
26	Информационная безопасность
27	Азартные игры, лотереи, тотализаторы
28	Общение в сети
29	Спам-сайты
30	Транспорт
31	Искусство
32	Криптовалюты, майнинг
33	Запрещено законодательством Бельгии
34	Интернет-магазины, банки, платежные системы
35	Видеоигры
36	Религии, религиозные объединения
37	Новостные ресурсы
38	Порнография, эротика
39	Нудизм
40	Белье
41	Секс-образование

42	Знакомства для взрослых
43	ЛГБТ+
44	Интим-магазины
45	Наркотики
46	Алкоголь
47	Табак
48	Культура, общество
49	Власть, политика, закон
50	Дом, семья
51	Вооруженные силы
52	Рестораны, кафе, еда
53	Астрология, эзотерика
54	Торренты
55	Файловые обменники
56	Аудио, видео
57	Информационные технологии
58	Поисковые машины и сервисы
59	Хостинг
60	Реклама, тизерные сети
61	Банки
62	Недвижимость
63	Фишинговые веб-сайты
64	Вредоносные веб-сайты
65	Самоповреждение, самоубийство
66	Блоги
67	Сайты знакомств
68	Образование
69	Школы, университеты
70	Книги, писатели
71	Образовательные порталы, базы знаний
72	Хобби, развлечения
73	Охота, рыбалка
74	Путешествия, поездки
75	ТВ, радио

76	Дикие и домашние животные
77	Юмор
78	Музыка
79	Красота, здоровье, спорт
80	Спорт, спортивные игры
81	Здоровье
82	Мода, стиль
83	Медицина, фармацевтика
84	Лотереи
85	Казино, карточные игры
86	Онлайн-тотализаторы
87	Ненависть, дискриминация
88	Экстремизм, расизм
89	Другие
90	Анорексия
91	Аборты
92	Детский интернет
93	Интернет-сервисы
94	Запрещено законодательством Российской Федерации
95	ФЗ РФ № 436
96	Федеральный список экстремистских материалов, действующий в РФ
97	Список Роскомнадзора РФ
98	Запрещено региональным законодательством
112	Ресурсы, обработанные компонентом SystemControlChanges
113	Рекламные программы
114	Потенциально опасные программы
115	IP-адреса, на которых расположены только вредоносные домены
116	Ресурсы, обработанные компонентом SystemControlChangesUBI
117	Ресурсы, в ходе посещения которых выполняется загрузка вредоносного программного кода
118	Ресурсы, содержащие, помимо основного контента, вредоносное программное обеспечение и используемые злоумышленниками при проведении атак
122	Узлы Tor
123	Динамический DNS
124	Средства удаленного администрирования

130	Военные игры
136	Рекламные программы
137	Разрешенный веб-сайт (локальная репутационная база организации)
138	Запрещенный веб-сайт (локальная репутационная база организации)
142	Ложные фишинговые веб-сайты

kaspersky

Глоссарий

A

Anti-Spam

Сервис предоставляет программам защиты почтовых серверов "Лаборатории Касперского" данные для фильтрации почтового потока от нежелательных сообщений (спама).

C

Cloud Information

Сервис предоставляет программам "Лаборатории Касперского" информацию о показателях баз репутации файлов. В программе "Лаборатории Касперского" может отображаться количество опасных, безопасных и других файлов.

F

File Reputation

Сервис предоставляет программам "Лаборатории Касперского" информацию о безопасных и опасных файлах и отображает сведения о категории файла (например, компьютерная игра). Кроме того, сервис предоставляет программе "Лаборатории Касперского" сведения о частоте обнаружения файла во всех странах мира и о географическом распространении файла.

G

Gateway Input

Компонент получает пакеты с репутационными базами от Kaspersky Security Network, проверяет целостность данных, упаковывает данные в файлы и отправляет файлы в категорированный сегмент сети.

Gateway Output

Компонент получает файлы с данными из открытого сегмента сети и распаковывает их.

K

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, 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.

M

MD5

Контрольная сумма MD5 (Message Digest 5) – это уникальный идентификатор файла. MD5 вычисляется с помощью 128-битного алгоритма хеширования и используется для проверки целостности файла. Для вычисления MD5 файлов предназначено много программ и сервисов.

Monitoring System

Компонент Monitoring System позволяет администратору Kaspersky Private Security Network через веб-интерфейс устанавливать компоненты Kaspersky Private Security Network на серверы, удаленно управлять этими серверами, осуществлять мониторинг их работоспособности, следить за быстродействием и качеством связи между серверами и компьютерами пользователей, а также управлять учетными записями администраторов Kaspersky Private Security Network.

P

Proxy

Компонент Proxy получает пакеты с репутационными базами с серверов "Лаборатории Касперского" и отправляет эти пакеты в категорированный сегмент сети.

R

Record Management

Сервис предоставляет антивирусным программам информацию об отзыве вирусными аналитиками "Лаборатории Касперского" отдельных вирусных записей в локальных базах антивирусных программ. Сервис используется для быстрой обработки изменений оценки программ с "опасная" на "безопасная". Запись о том, что программу следует считать вредоносной, хранится в локальной базе антивирусной программы. Если оценка была изменена, сервис Kaspersky Private Security Network оперативно обновляет запись в базе антивирусной программы.

S

SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

U

URL Reputation

Сервис предоставляет антивирусной программе информацию об опасных и безопасных веб-сайтах. Кроме того, сервис отображает сведения о категории веб-сайта (например, Для взрослых).

kaspersky

А

Атака "нулевого дня"

Атака на IT-инфраструктуру организации, использующая уязвимости "нулевого дня" в программном обеспечении, которые становятся известны злоумышленникам до момента выпуска производителем программного обеспечения обновления, содержащего исправления.

К

Категории "Лаборатории Касперского"

Готовые категории данных, разработанные сотрудниками "Лаборатории Касперского". Категории могут обновляться при обновлении баз программы. Специалист по информационной безопасности не может изменять или удалять готовые категории.

Категорированный сегмент сети

Участок локальной сети, с которого запрещен доступ в интернет и в другие сегменты локальной сети.

Ключ шифрования трафика

Уникальная буквенно-цифровая последовательность. Ключ используется для шифрования данных, передаваемых между серверами Kaspersky Private Security Network и компьютерами, на которых установлены программы "Лаборатории Касперского". Закрытая часть ключа шифрования трафика хранится на серверах Kaspersky Private Security Network. Открытая часть ключа шифрования подписывается в "Лаборатории Касперского", а затем копируется на компьютеры пользователей с установленными программами "Лаборатории Касперского".

О

Однонаправленный шлюз

Устройство, предназначенное для однонаправленной передачи данных из открытого сегмента сети в категорированный сегмент сети.

Открытый сегмент сети

Участок локальной сети, с которого открыт доступ в интернет и в другие сегменты локальной сети.

С

Спам

Несанкционированная массовая рассылка сообщений электронной почты, чаще всего рекламного характера.

kaspersky

Ц

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.

Э

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы "Лаборатории Касперского". Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

kaspersky

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com (https://community.kaspersky.com/)

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в директории /usr/local/ksn на компьютере с установленным компонентом Monitoring System.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Mac – товарный знак Apple Inc., зарегистрированный в США и других странах.

Google Chrome и Android – товарные знаки Google, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

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

Mozilla и Firefox – товарные знаки Mozilla Foundation.

Pivotal и RabbitMQ – товарные знаки и/или зарегистрированные в США и/или других странах товарные знаки Pivotal Software, Inc.

Tor – товарный знак The Tor Project, регистрация в США № 3 465 432.

Zabbix – зарегистрированный товарный знак Zabbix SIA.

kaspersky

Предметный указатель

A

F

G

K

M

U

M

O

У