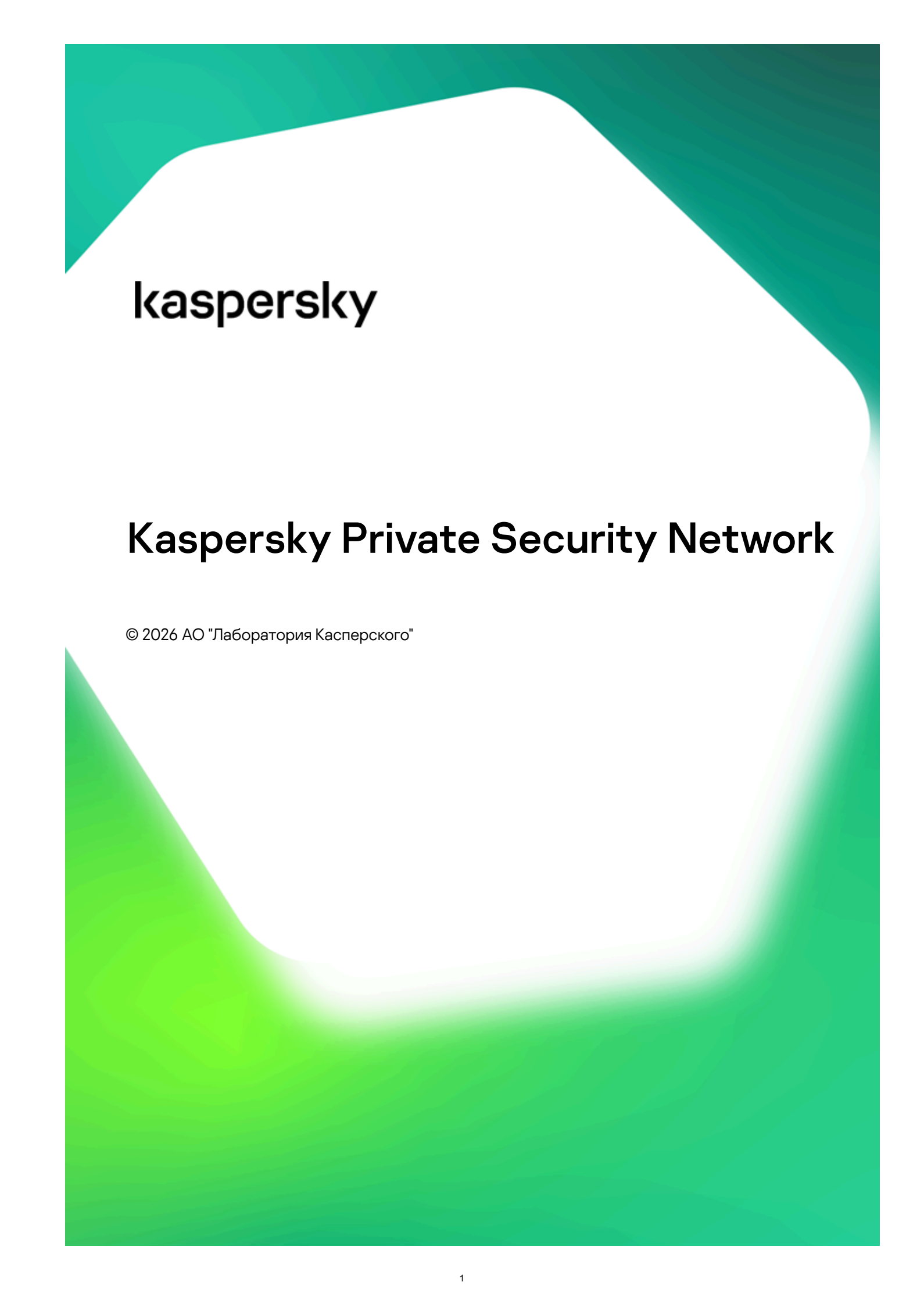


The background of the entire page is a vibrant green with a subtle gradient. A large, white, rounded rectangular shape is centered on the page, creating a frame for the text. The Kaspersky logo is positioned in the upper left of this white area.

kaspersky

Kaspersky Private Security Network

© 2026 АО "Лаборатория Касперского"

Содержание

[О Kaspersky Private Security Network](#)

[О Kaspersky Security Network](#)

[Об отличиях Kaspersky Private Security Network от Kaspersky Security Network](#)

[Что нового в версии 4.0](#)

[Комплект поставки](#)

[Лицензирование Kaspersky Private Security Network](#)

[Аппаратные и программные требования](#)

[Архитектура приложения](#)

[Типовые схемы развертывания](#)

[Простые схемы развертывания](#)

[Развертывание Kaspersky Private Security Network с резервированием](#)

[Управление правами доступа](#)

[Добавление и удаление сервера](#)

[Установка Kaspersky Private Security Network](#)

[Подготовка к установке Kaspersky Private Security Network](#)

[Установка серверной части Kaspersky Private Security Network](#)

[Получение файла интеграции с веб-плагином Kaspersky Private Security Network](#)

[Установка веб-плагина Kaspersky Private Security Network](#)

[Шаг 1. Интеграция серверной части Kaspersky Private Security Network и веб-плагина Kaspersky Private Security Network](#)

[Шаг 2. Загрузка активационного архива](#)

[Шаг 3. Выбор компонентов для установки](#)

[Шаг 4. Установка компонентов](#)

[Шаг 5. Добавление ключей шифрования трафика](#)

[Шаг 6. Добавление идентификатора установки](#)

[Шаг 7. Проверка конфигурации](#)

[Завершение установки](#)

[Обновление Kaspersky Private Security Network](#)

[Обновление веб-плагина Kaspersky Private Security Network](#)

[Обновление серверной части Kaspersky Private Security Network](#)

[Обновление Kaspersky Private Security Network до версии 4.01](#)

[Обновление Kaspersky Private Security Network до версии 4.0.2](#)

[Обновление Kaspersky Private Security Network до версии 4.0.3](#)

[Обновление Kaspersky Private Security Network до версии 4.0.4](#)

[Обновление Kaspersky Private Security Network до версии 4.0.5](#)

[Обновление Kaspersky Private Security Network до версии 4.0.6](#)

[Удаление интеграции с Kaspersky Private Security Network](#)

[Удаление Kaspersky Private Security Network](#)

[Сертификат для получения обновлений](#)

[Обновление баз](#)

[Запрос на обновление баз](#)

[Контроль обновления баз](#)

[Устранение сбоев передачи данных через однонаправленный шлюз](#)

[Настройка прокси-сервера](#)

[Конфигурация Kaspersky Private Security Network](#)

[Просмотр информации о конфигурации](#)

[Добавление и удаление компонентов](#)

[Получение конфигурационных файлов Kaspersky Private Security Network](#)

[Шифрование трафика](#)

[Создание ключа шифрования трафика](#)

[Добавление ключа шифрования трафика](#)

[Экспорт и импорт хранилища ключей шифрования трафика](#)

[Адреса доступа к сервисам Kaspersky Private Security Network](#)

[Управление локальными репутационными базами](#)

[Добавление и обновление сведений о репутации файлов или веб-сайтов](#)

[Экспорт локальной репутационной базы в текстовый файл](#)

[Удаление записей о репутации файлов или веб-сайтов](#)

[Мониторинг работы Kaspersky Private Security Network](#)

[Мониторинг состояния компонентов и серверов](#)

[Мониторинг репутации объектов](#)

[Мониторинг времени обработки запросов](#)

[Мониторинг отставания обновляемых баз](#)

[Устранение неполадок в работе компонентов Kaspersky Private Security Network](#)

[Оповещения о событиях в работе Kaspersky Private Security Network](#)

[Настройка почтовых оповещений о событиях в работе Kaspersky Private Security Network](#)

[Настройка записи в Syslog событий в работе Kaspersky Private Security Network](#)

[API KPSN](#)

[Подготовка к использованию API](#)

[Выполнение запросов к API](#)

[Добавление сведений о репутации файла](#)

[Добавление сведений о репутации веб-сайта](#)

[Удаление сведений о репутации файла](#)

[Удаление сведений о репутации веб-сайта](#)

[Проверка репутации файлов](#)

[Проверка репутации веб-сайтов](#)

[Коды ошибок](#)

[Журнал Kaspersky Private Security Network](#)

[Включение и выключение записи запросов для сервисов URL Reputation и File Reputation](#)

[Обращение в Службу технической поддержки](#)

[Способы получения технической поддержки](#)

[Техническая поддержка через Kaspersky CompanyAccount](#)

[Приложения](#)

[Список портов для работы Kaspersky Private Security Network](#)

[Список категорий веб-сайтов сервиса URL Reputation](#)

[Обновление стороннего программного обеспечения, используемого Kaspersky Private Security Network 4.0.3 и выше](#)

[Обновление стороннего программного обеспечения](#)

[Обновление стороннего программного обеспечения в конфигурации с однонаправленным шлюзом](#)

[Возврат стороннего программного обеспечения к версиям, используемым Kaspersky Private Security Network по умолчанию](#)

[Источники информации о программе](#)

[Глоссарий](#)

[Anti-Spam](#)

[Cloud Information](#)

[File Reputation](#)

[Gateway External](#)

[Gateway Internal](#)

[Kaspersky Security Network \(KSN\)](#)

[MD5](#)

[Record Management](#)

[SSL](#)

[URL Reputation](#)

[Категории "Лаборатории Касперского"](#)

[Категорированный сегмент сети](#)

[Ключ шифрования трафика](#)

[Однонаправленный шлюз](#)

[Открытый сегмент сети](#)

[Спам](#)

[Информация о стороннем коде](#)

[Уведомления о товарных знаках](#)

О Kaspersky Private Security Network

Kaspersky Private Security Network – это решение, позволяющее пользователям компьютеров, на которые установлены приложения "Лаборатории Касперского" (далее "компьютеры организации"), получать доступ к репутационным базам [Kaspersky Security Network](#), а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.

Решение Kaspersky Private Security Network (далее также *KPSM*) разработано для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например по следующим причинам:

- отсутствие подключения локальных рабочих мест к сети Интернет;
- требования корпоративной безопасности или законодательный запрет на отправку любых данных за пределы страны или за пределы локальной сети организации.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

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

- Kaspersky Anti Targeted Attack Platform.
- Kaspersky Security Center.
- Kaspersky Endpoint Detection and Response
- Kaspersky Secure Mail Gateway.
- Kaspersky Web Filter Software Development Kit.
- Kaspersky Web Traffic Security.
- Начиная с Kaspersky Private Security Network 4.0.5: Kaspersky Anti-Virus Software Development Kit Level 3 для Windows® версии 8.10.2 и выше.
- Начиная с Kaspersky Private Security Network 4.0.6: Kaspersky Anti-Virus Software Development Kit Level 3 для Linux® версии 8.10.4 и выше.
- Начиная с Kaspersky Private Security Network 4.0.6: Kaspersky Anti-Virus Software Development Kit Level 3 для Mac® версии 8.10.4 и выше.

Kaspersky Private Security Network совместно с Kaspersky Security Center может использоваться со следующими приложениями "Лаборатории Касперского":

- Kaspersky Embedded Systems Security.
- Kaspersky Endpoint Security for Android™.
- Kaspersky Endpoint Security для Linux.
- Kaspersky Endpoint Security для Mac.

- Kaspersky Endpoint Security для Windows.
- Kaspersky Industrial Cyber Security for Nodes.
- 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.

Подробную информацию об использовании Kaspersky Private Security Network с приложениями "Лаборатории Касперского" см. в документации к этим приложениям.

Вы можете использовать Kaspersky Private Security Network в следующих конфигурациях:

- **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 использованием прокси-сервера**

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 с серверами "Лаборатории Касперского" осуществляется через прокси-сервер сети вашей организации.

- **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 [однаправленного шлюза](#).

Конфигурация Kaspersky Private Security Network определяется корпоративными требованиями безопасности.

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 приложений "Лаборатории Касперского" во всем мире;
- отзывах вирусными аналитиками "Лаборатории Касперского" отдельных вирусных записей в локальных базах антивирусных приложений (например, изменение оценки объекта с "опасный" на "безопасный").

Данные Kaspersky Security Network используются в приложениях "Лаборатории Касперского" для следующих целей:

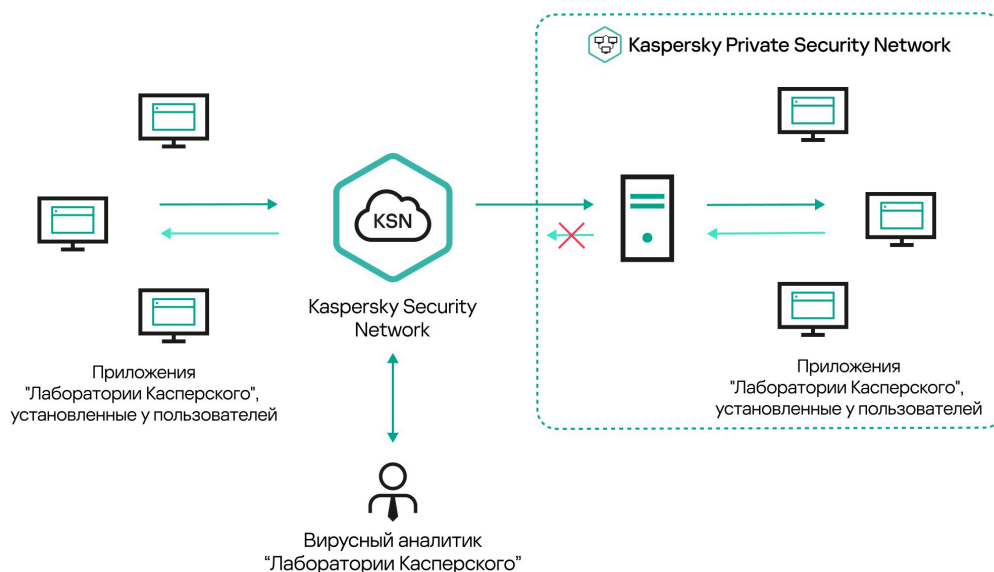
- предоставления актуальной информации об объектах, ещё не вошедших в базы вредоносного ПО;
- снижения вероятности ложных срабатываний Анти-Спама;
- блокирования доступа пользователя к вредоносным веб-сайтам;
- блокирования запуска вредоносных файлов на компьютере пользователя;
- ограничения доступа 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, приложение "Лаборатории Касперского", установленное 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.



Сравнение принципов работы Kaspersky Security Network и Kaspersky Private Security Network

Что нового в версии 4.0

Kaspersky Private Security Network 4.0

В Kaspersky Private Security Network версии 4.0 появились следующие возможности и доработки:

- Обновлен пользовательский интерфейс Kaspersky Private Security Network: теперь Kaspersky Private Security Network является веб-плагином в составе веб-интерфейса Kaspersky Security Center Web Console.
- Добавлен мастер настройки Kaspersky Private Security Network.
- Добавлена поддержка использования прокси-сервера организации.
- Файлы с параметрами подключения к серверам службы Kaspersky Private Security Network можно получить через веб-интерфейс.
- Обновления репутационной базы файлов для работы сервиса File Reputation содержат записи, идентифицирующие файлы как по MD5-хешу, так и по SHA256-хешу.

Kaspersky Private Security Network 4.0.1

В Kaspersky Private Security Network версии 4.0.1 появились следующие возможности и доработки:

- Обновлён выбор отображаемого интервала времени для графиков.
- Для компонентов Gateway Internal и Gateway External в интерфейсе добавлено отображение сервера, на котором установлен компонент.

Kaspersky Private Security Network 4.0.2

В Kaspersky Private Security Network версии 4.0.2 исправлены ошибки, выявленные в версиях 4.0 и 4.0.1.

Kaspersky Private Security Network 4.0.3

В Kaspersky Private Security Network версии 4.0.3 появились следующие возможности и доработки:

- Обновлены версии используемого стороннего кода.
- Добавлена возможность [обновления версий контейнеров используемого стороннего программного обеспечения](#).

Kaspersky Private Security Network 4.0.4

В Kaspersky Private Security Network версии 4.0.4 появились следующие возможности и доработки:

- Добавлена поддержка новых версий оркестратора K3s.
- Добавлена поддержка Red Hat Enterprise Linux 9.6.

Kaspersky Private Security Network 4.0.5

В Kaspersky Private Security Network версии 4.0.5 появились следующие возможности и доработки:

- Поддержана совместимость с новыми версиями стороннего программного обеспечения.
- Поддержана совместимость с KAV SDK L3 for Windows, начиная с версии 8.10.3.

Kaspersky Private Security Network 4.0.6

В Kaspersky Private Security Network версии 4.0.6 появились следующие возможности и доработки:

- Поддержана совместимость с новыми версиями стороннего программного обеспечения.
- Улучшен мониторинг работы компонентов.

Комплект поставки

В комплект поставки Kaspersky Private Security Network входят следующие компоненты:

- установочный архив веб-плагина Kaspersky Private Security Network для Kaspersky Security Center;
- установочный архив серверной части Kaspersky Private Security Network;
- Release Notes Kaspersky Private Security Network.

Лицензирование Kaspersky Private Security Network

О Лицензионном соглашении

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

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с Kaspersky Private Security Network.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- При установке серверной части Kaspersky Private Security Network.
- На сервере с установленной серверной частью Kaspersky Private Security Network, с помощью команды `kpsnctl show-eula`

Утилита `kpsnctl` находится в установочном архиве серверной части Kaspersky Private Security Network.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения при установке серверной части KPSN, а именно, указывая параметр `--accept-eula` при запуске установки. Если вы не согласны с условиями Лицензионного соглашения, вы не должны использовать Kaspersky Private Security Network.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Private Security Network, предоставляемое вам на основании Лицензионного соглашения.

Срок действия лицензии равен сроку действия [сертификата для получения обновлений](#).

Лицензия включает в себя право на получение следующих услуг:

- Использование веб-плагина и серверной части Kaspersky Private Security Network.
- Обращение в Службу технической поддержки "Лаборатории Касперского".
- Получение прочих услуг, предоставляемых вам "Лабораторией Касперского" или ее партнерами в течение срока действия лицензии.

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

- **Kaspersky Private Security Network Standard**
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).

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 приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);

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

Аппаратные и программные требования

Программные требования для установки серверной части Kaspersky Private Security Network

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

Kaspersky Private Security Network версии 4.0–4.0.3

На каждом из серверов, предназначенных для установки компонентов Kaspersky Private Security Network, должно быть установлено следующее программное обеспечение:

- Операционная система: Ubuntu 24.04 LTS.
- Helm® версии 3.x.x, не ранее 3.15.3.
- Оркестратор K3s следующих версий:
 - 1.29.1–1.29.15.
 - 1.30.0–1.30.14.
 - 1.31.0–1.31.5.
 - 1.32.0–1.32.1.

В оркестраторе K3s необходимо отключить использование компонента traefik.

Серверы должны быть объединены в Kubernetes®-кластер под управлением оркестратора K3s.

Kaspersky Private Security Network использует весь кластер.

Средствами Kubernetes возможно добавление серверов в кластер после установки Kaspersky Private Security Network.

Kaspersky Private Security Network версии 4.0.4

На каждом из серверов, предназначенных для установки компонентов Kaspersky Private Security Network, должно быть установлено следующее программное обеспечение:

- Операционная система: Ubuntu 24.04 LTS или Red Hat Enterprise Linux 9.6.
- Helm® версии 3.x.x, не ранее 3.15.3.
- Оркестратор K3s следующих версий:
 - 1.29.1–1.29.15.
 - 1.30.0–1.30.14.
 - 1.31.0–1.31.13.
 - 1.32.0–1.32.9.
 - 1.33.0–1.33.5.
 - 1.34.1.

В оркестраторе K3s необходимо отключить использование компонента traefik.

Серверы должны быть объединены в Kubernetes®-кластер под управлением оркестратора K3s.

Kaspersky Private Security Network использует весь кластер.

Средствами Kubernetes возможно добавление серверов в кластер после установки Kaspersky Private Security Network.

Kaspersky Private Security Network версии 4.0.5

На каждом из серверов, предназначенных для установки компонентов Kaspersky Private Security Network, должно быть установлено следующее программное обеспечение:

- Операционная система: Ubuntu 24.04 LTS или Red Hat Enterprise Linux 9.6.
- Helm® версии 3.19.0 и выше.
- Оркестратор K3s следующих версий:
 - 1.32.2–1.32.13.
 - 1.33.0–1.33.9.
 - 1.34.1–1.34.5.
 - 1.35.0–1.35.2.

В оркестраторе K3s необходимо отключить использование компонента traefik.

Серверы должны быть объединены в Kubernetes®-кластер под управлением оркестратора K3s.

Kaspersky Private Security Network использует весь кластер.

Средствами Kubernetes возможно добавление серверов в кластер после установки Kaspersky Private Security Network.

Kaspersky Private Security Network версии 4.0.6

На каждом из серверов, предназначенных для установки компонентов Kaspersky Private Security Network, должно быть установлено следующее программное обеспечение:

- Операционная система: Ubuntu 24.04 LTS, Red Hat Enterprise Linux 9.8.
- Helm® 4.1.1 и оркестратор K3s 1.35.2 или Helm 4.3.0 и оркестратор K3s 1.36.4.
В оркестраторе K3s необходимо отключить использование компонента traefik.

Серверы должны быть объединены в Kubernetes®-кластер под управлением оркестратора K3s.

Kaspersky Private Security Network использует весь кластер.

Средствами Kubernetes возможно добавление серверов в кластер после установки Kaspersky Private Security Network.

Аппаратные требования для установки серверной части Kaspersky Private Security Network

Аппаратные требования к серверам, входящим в кластер, представлены в таблицах ниже. Компоненты Kaspersky Private Security Network распределяются по серверам внутри кластера автоматически. Компоненты устанавливаются в соответствии [со схемой развертывания](#).

Схема развертывания	Установленные компоненты	Аппаратные требования
Стандартная	- File Reputation. - URL Reputation. - Anti-Spam. - Cloud Information. - Certificate Validation. - RMS.	- Процессор – 2,8 ГГц, 16 ядер. - Объем оперативной памяти – 116 ГБ. - Дисковая подсистема – 1 ТБ SSD (не менее 50 000 операций чтения/записи в секунду). - Для работы с локальной репутационной базой сервиса File Reputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства. - Для работы с локальной репутационной базой сервиса URL Reputation требуется дополнительное свободное пространство. Для каждого 1 млн записей требуется 2 ГБ дискового пространства и 0,5 ГБ оперативной памяти.
С однонаправленным шлюзом	Кластер в открытом сегменте: Gateway External.	- Процессор – 2 ГГц, 4 ядра. - Объем оперативной памяти – 16 ГБ. - Дисковая подсистема – 72 ГБ свободного пространства.
	Кластер в категоризованном сегменте: - Gateway Internal. - File Reputation. - URL Reputation. - Anti-Spam. - Cloud Information. - Certificate Validation. - RMS.	- Процессор – 2,8 ГГц, 16 ядер. - Объем оперативной памяти – 116 ГБ. - Дисковая подсистема – 1,5 ТБ SSD (не менее 50 000 операций чтения/записи в секунду). - 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.
	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. После настройки дополнительной защиты убедитесь, что соединения, необходимые для работы приложения, доступны.

Программные требования для установки веб-плагина

Плагин должен быть установлен на сервер с установленным Kaspersky Security Center Kaspersky Security Center Web Console. Поддерживаемые версии Kaspersky Security Center:

- Kaspersky Security Center 14.2 Windows.
- Kaspersky Security Center 15.1 Windows.
- Kaspersky Security Center 15 Linux.
- Kaspersky Security Center 15.1 Linux.
- Kaspersky Security Center 15.2 Linux.
- Kaspersky Security Center 15.3 Linux.
- Kaspersky Security Center 15.4 Linux.
- Kaspersky Security Center 16 Linux.

- Kaspersky Security Center 16.1 Linux.
- Kaspersky Security Center 16.2 Linux.
- Kaspersky Security Center 16.3 Linux.
- Kaspersky Security Center 17 Linux.

На компьютере, предназначенном для работы с веб-плагином Kaspersky Private Security Network, должен быть установлен браузер. Ограничений по использованию типов и версий браузеров не предусмотрено. Рекомендуется использовать браузеры Google™ Chrome™, Mozilla™ Firefox™ или Microsoft® Edge.

Аппаратные требования для установки веб-плагина

Аппаратные требования к серверу Kaspersky Security Center, на который будет установлен веб-плагин Kaspersky Private Security Network, соответствуют аппаратным требованиям Kaspersky Security Center. Подробнее см. в *справке Kaspersky Security Center*.

Архитектура приложения

Работа Kaspersky Private Security Network обеспечивается следующими основными компонентами:

- Веб-плагин Kaspersky Private Security Network предоставляет веб-интерфейс для управления Kaspersky Private Security Network и работы с ним. Взаимодействие между серверной частью Kaspersky Private Security Network и веб-плагином осуществляется по зашифрованному каналу связи.

Веб-плагин Kaspersky Private Security Network [устанавливается вручную](#) в Kaspersky Security Center Web Console.

На компьютерах, с которых будет осуществляться управление Kaspersky Private Security Network через веб-плагин в Kaspersky Security Center Web Console, должен быть установлен [поддерживаемый браузер](#). Эти компьютеры также должны иметь доступ к серверам, на которых установлено приложение Kaspersky Security Center Web Console.

- Серверная часть Kaspersky Private Security Network, включающая в себя следующие компоненты:

- **Gateway External**

Компонент Gateway External обеспечивает обновление репутационных баз компонентов Kaspersky Private Security Network в конфигурации с использованием однонаправленного шлюза.

Компонент Gateway External выполняет следующие функции:

- получение пакетов с репутационными базами для компонентов Kaspersky Private Security Network с серверов "Лаборатории Касперского";
- проверка целостности принятых данных;
- упаковка и отправка пакетов с репутационными базами через однонаправленный шлюз в категоризованный сегмент сети на сервер с компонентом Gateway Internal.

Компонент Gateway External устанавливается в открытом сегменте сети.

- **Gateway Internal**

Компонент Gateway Internal обеспечивает обновление репутационных баз компонентов Kaspersky Private Security Network в конфигурации с использованием однонаправленного шлюза.

Компонент Gateway Internal выполняет следующие функции:

- получение и распаковка упакованных пакетов с репутационными базами через однонаправленный шлюз с сервера с компонентом Gateway External, расположенного в открытом сегменте сети;
- проверка целостности принятых данных;
- обновление репутационных баз компонентов Kaspersky Private Security Network на серверах категоризованного сегмента сети.

Компонент Gateway Internal устанавливается на сервер в категоризованном сегменте сети.

- **Cloud Information**

Компонент Cloud Information предоставляет приложениям "Лаборатории Касперского" информацию об общих показателях баз данных репутации объектов.

На основе информации от компонента приложения "Лаборатории Касперского" могут отображать, например, количество объектов с определенной репутацией (опасные, безопасные и другие).

- **File Reputation**

Компонент File Reputation предоставляет приложениям "Лаборатории Касперского" следующую информацию:

- репутация файлов;
- категория файла (например, файл операционной системы);
- частота обнаружения файла во всех странах мира и географическое распространение файла.

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

- **URL Reputation**

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

На основании информации от компонента приложения "Лаборатории Касперского" могут блокировать доступ к вредоносным веб-сайтам на компьютерах пользователей и ограничивать доступ к отдельным категориям веб-сайтов.

- **Certificate Validation**

Компонент Certificate Validation предоставляет приложениям "Лаборатории Касперского" информацию о репутации файлов на основе репутации сертификатов, которыми они подписаны. Если файл подписан сертификатом из доверенного источника, этот файл также считается доверенным. Например, приложение считается доверенным, если оно подписано сертификатом, предоставленным официальным магазином.

На основании этой информации приложения "Лаборатории Касперского" могут определять репутацию файлов, которые подписаны сертификатами (доверенный или недоверенный).

- **Anti-Spam**

Компонент Anti-Spam предоставляет приложениям защиты почтовых серверов "Лаборатории Касперского" статистические данные для защиты и фильтрации почтового потока от нежелательных сообщений (спам). Подробнее о работе приложений защиты почтовых серверов см. [в документации к этим приложениям](#) ^[2].

- **Record Management System (RMS)**

Компонент RMS предоставляет антивирусным приложениям "Лаборатории Касперского" информацию о репутации объектов. Информация поступает от вирусных аналитиков "Лаборатории Касперского".

Компонент используется для быстрой обработки изменений оценки объектов с "доверенный" на "недоверенный". Компонент RMS отслеживает сведения о репутации объектов и в случае изменений обновляет информацию об этом объекте в антивирусных базах данных, используемых приложениями "Лаборатории Касперского".

Серверная часть Kaspersky Private Security Network разворачивается в кластере Kubernetes в сети организации. Серверы должны соответствовать [аппаратным и программным требованиям](#). Архитектура Kaspersky Private Security Network и наличие или отсутствие компонентов серверной части зависят от [конфигурации приложения](#).

Вы можете выбрать нужные серверные компоненты при [установке веб-плагина Kaspersky Private Security Network в Kaspersky Security Center Web Console](#). Вы можете просмотреть информацию об установленных компонентах Kaspersky Private Security Network [в веб-интерфейсе Kaspersky Security Center Web Console](#).

Для обеспечения безопасной передачи данных между Kaspersky Private Security Network и приложениями в локальной сети организации требуется [добавить ключ шифрования трафика](#).

Взаимодействие между Kaspersky Private Security Network и Kaspersky Security Network осуществляется по зашифрованному каналу с использованием клиентского сертификата для авторизации, который предоставляется отдельно.

Утилита kpsnctl позволяет администратору управлять интеграцией серверной части Kaspersky Private Security Network и веб-плагина, корневым сертификатом в иерархии сертификатов Kaspersky Private Security Network и сертификатом сервера. С помощью утилиты kpsnctl администратор также может просматривать [Лицензионное соглашение Kaspersky Private Security Network](#).

Типовые схемы развертывания

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

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

Простые схемы развертывания

Простые схемы развертывания предполагают развертывание компонентов Kaspersky Private Security Network в одном экземпляре.

Kaspersky Private Security Network может быть развернут в следующих конфигурациях:

- стандартная;
- с использованием прокси-сервера;
- с однонаправленным шлюзом.

Выбор конфигурации Kaspersky Private Security Network определяется требованиями корпоративной безопасности вашей организации.

Стандартная конфигурация Kaspersky Private Security Network

Стандартная конфигурация Kaspersky Private Security Network используется, если все серверы, на которых установлены компоненты Kaspersky Private Security Network, имеют доступ к серверам "Лаборатории Касперского".

Для развертывания серверной части Kaspersky Private Security Network в стандартной конфигурации требуется:

- Кластер, на который необходимо установить все компоненты сервера Kaspersky Private Security Network, кроме компонентов Gateway External и Gateway Internal.

Компоненты Gateway External и Gateway Internal используются только в конфигурации с однонаправленным шлюзом.

- Сервер с установленным Kaspersky Security Center, в котором будет установлен веб-плагин Kaspersky Private Security Network. Подробнее см. [Аппаратные и программные требования](#).

Схема развертывания Kaspersky Private Security Network в стандартной конфигурации представлена на рис. ниже.

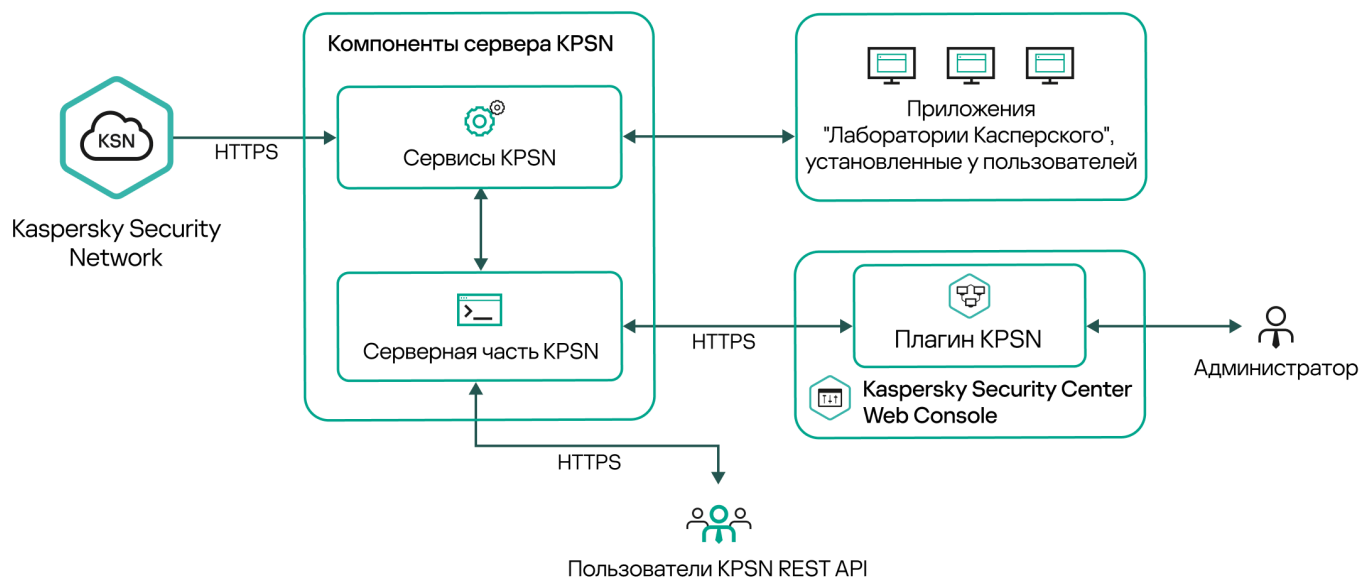


Схема развертывания Kaspersky Private Security Network в стандартной конфигурации

Kaspersky Private Security Network с использованием прокси-сервера

Конфигурация Kaspersky Private Security Network с использованием прокси-сервера используется, если в локальной сети организации доступ к серверам "Лаборатории Касперского" разрешен только с использованием прокси-сервера, предоставляемого вашей организацией. В этом случае локальная сеть организации разделяется на [открытый](#) и [категоризированный](#) сегменты сети, на одном из которых находится прокси-сервер, а на другом – Kaspersky Private Security Network.

Для развертывания серверной части Kaspersky Private Security Network с использованием прокси-сервера требуется:

- Кластер, расположенный в категоризованном сегменте сети. На серверы кластера необходимо установить все компоненты серверной части Kaspersky Private Security Network, кроме компонентов Gateway External и Gateway Internal.

Компоненты Gateway External и Gateway Internal используются только в конфигурации с однонаправленным шлюзом.

- Сервер, расположенный в открытом сегменте сети, на котором развернут прокси-сервер вашей организации.
- Сервер, расположенный в категоризованном сегменте сети. На этом сервере необходимо развернуть все компоненты Kaspersky Private Security Network, кроме компонентов Gateway External и Gateway Internal.
- Сервер с установленным Kaspersky Security Center, в котором будет установлен веб-плагин Kaspersky Private Security Network. Подробнее см. [Аппаратные и программные требования](#).

Для обеспечения взаимодействия Kaspersky Private Security Network с серверами "Лаборатории Касперского" через прокси-сервер вашей организации необходимо настроить [параметры прокси-сервера](#) через веб-плагин Kaspersky Private Security Network.

Схема разворачивания Kaspersky Private Security Network с использованием прокси-сервера представлена на рис. ниже.

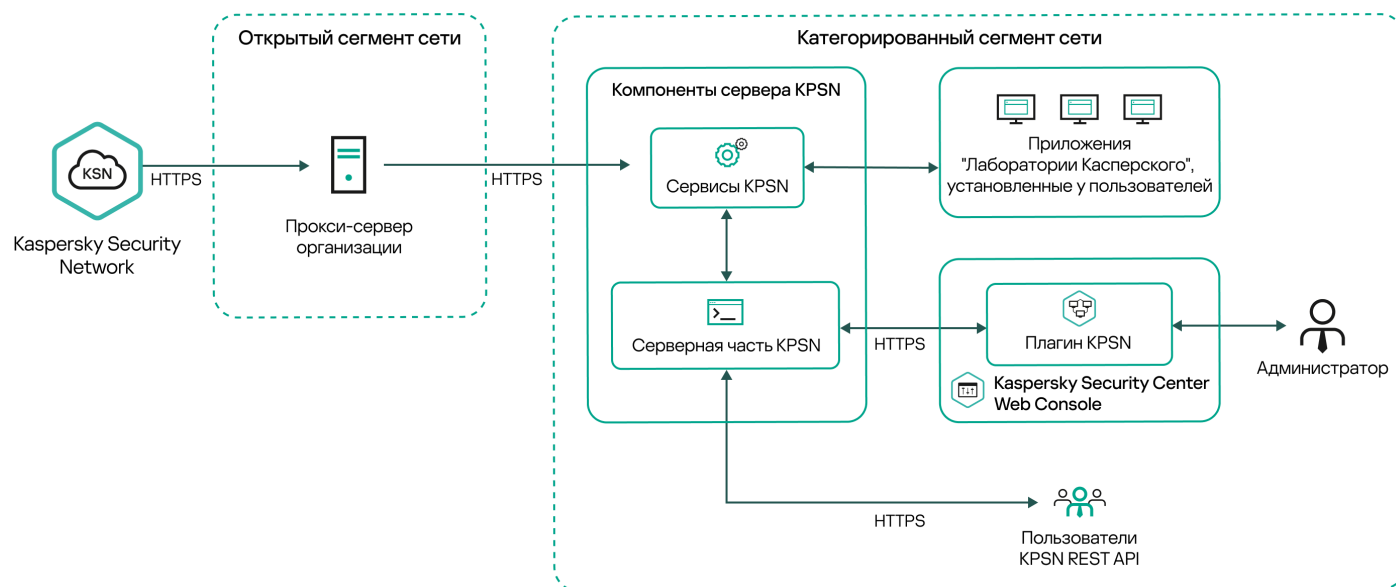


Схема разворачивания Kaspersky Private Security Network с использованием прокси-сервера

Kaspersky Private Security Network с однонаправленным шлюзом

Конфигурация Kaspersky Private Security Network с однонаправленным шлюзом используется, если в локальной сети организации запрещен доступ к серверам "Лаборатории Касперского". В этом случае локальная сеть организации разделяется на открытый и категорированный сегменты, взаимодействие между которыми осуществляется с помощью однонаправленного шлюза. В обоих сегментах сети необходимо установить Kaspersky Private Security Network и Kaspersky Security Center Web Console, но для Kaspersky Private Security Network в разных сегментах требуются разные компоненты.

Для разворачивания Kaspersky Private Security Network с однонаправленным шлюзом требуются минимум два кластера:

- **Кластер 1**, расположенный в открытом сегменте сети.

В кластере 1 необходимо развернуть серверную часть Kaspersky Private Security Network и компонент Gateway External. Компонент Gateway External может получать обновления репутационных баз с серверов "Лаборатории Касперского" по зашифрованному каналу связи.

- **Кластер 2**, расположенный в категорированном сегменте сети.

В кластере 2 необходимо развернуть серверную часть Kaspersky Private Security Network, компонент Gateway Internal и другие необходимые серверные компоненты Kaspersky Private Security Network. Компонент Gateway Internal может получать обновления репутационных баз от компонента Gateway External по однонаправленному шлюзу и передавать их в другие компоненты Kaspersky Private Security Network.

- Два сервера, на каждом из которых установлено приложение Kaspersky Security Center, в котором будет установлен веб-плагин Kaspersky Private Security Network. Подробнее см. [Аппаратные и программные требования](#). Один сервер должен располагаться в открытом сегменте сети, другой сервер должен располагаться в категорированном сегменте сети.

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

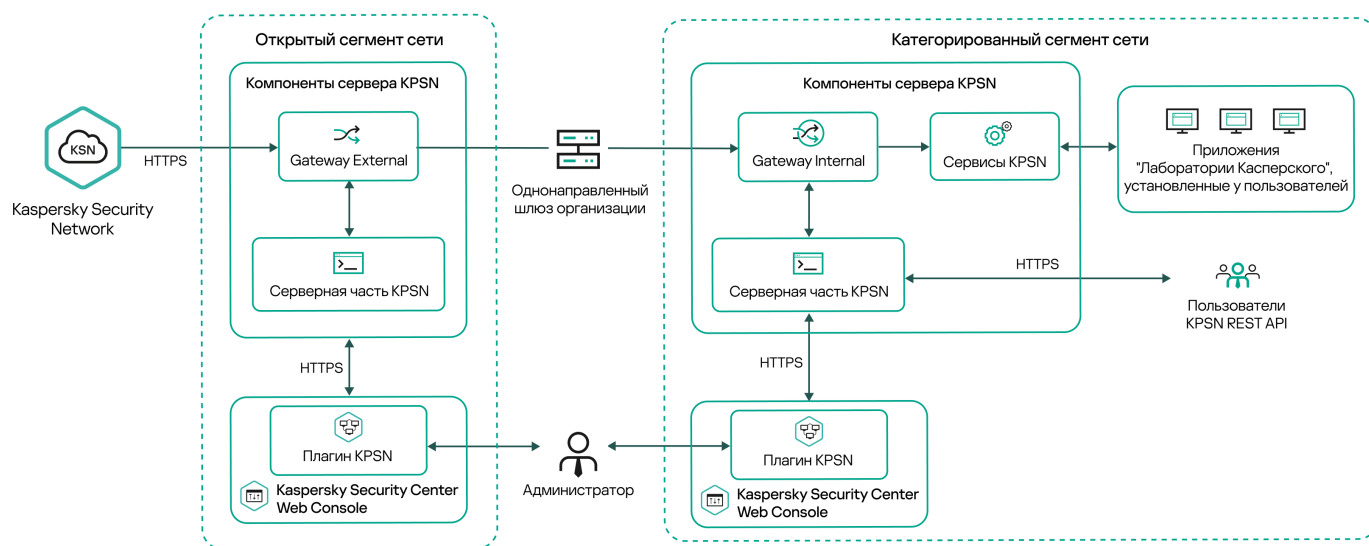


Схема развертывания Kaspersky Private Security Network с однонаправленным шлюзом

Развертывание Kaspersky Private Security Network с резервированием

Для повышения стабильности работы приложения вы можете установить несколько экземпляров компонентов Kaspersky Private Security Network. Например, вы можете добавить несколько экземпляров компонента URL Reputation при использовании [любой схемы развертывания](#) (стандартная, с использованием прокси-сервера или с однонаправленным шлюзом).

Максимальное количество экземпляров каждого компонента соответствует количеству серверов в кластере Kubernetes.
Компоненты Gateway External и Gateway Internal могут существовать только в одном экземпляре.

Вы можете [настроить количество экземпляров компонентов](#) через веб-плагин Kaspersky Private Security Network.

Управление правами доступа

Управление правами доступа к функциональности Kaspersky Private Security Network выполняется в Kaspersky Security Center Web Console (см. *справку Kaspersky Security Center*).

Для Kaspersky Private Security Network следует установить следующие права доступа:

- Доступ к API.
- Управление настройками Kaspersky Private Security Network.
- Управление локальной репутационной базой файлов.
- Управление локальной репутационной базой веб-сайтов.

Добавление и удаление сервера

Компоненты Kaspersky Private Security Network разворачиваются в кластере Kubernetes. Информацию о добавлении сервера в кластер см. в документации к оркестратору k3s.

Удаление сервера также происходит при помощи оркестратора. Перед удалением сервера убедитесь, что в результате удаления количество экземпляров каждого компонента не превысит количество оставшихся серверов в кластере.

После добавления или удаления сервера следует актуализировать [адреса доступа к сервисам Kaspersky Private Security Network](#):

- Добавить адрес добавленного сервера.
- Удалить адрес удалённого сервера.

Установка Kaspersky Private Security Network

Установка Kaspersky Private Security Network состоит из следующих этапов:

1. [Подготовка к установке Kaspersky Private Security Network](#)
2. [Установка серверной части Kaspersky Private Security Network.](#)
3. [Получение файла интеграции с веб-плагином Kaspersky Private Security Network.](#)
4. [Установка веб-плагина Kaspersky Private Security Network.](#)

В процессе установки веб-плагина выполняется его интеграция с серверной частью Kaspersky Private Security Network.

Подготовка к установке Kaspersky Private Security Network

Перед установкой Kaspersky Private Security Network требуется выполнить следующие действия:

1. Убедиться, что серверы находятся внутри локальной сети в соответствии со [схемой развертывания](#).
2. Убедиться, что серверы удовлетворяют [аппаратным и программным требованиям](#).
3. Убедиться, что разрешены [необходимые входящие и исходящие соединения](#).

Рекомендуется закрыть все порты, кроме перечисленных в разделе [Список портов для работы Kaspersky Private Security Network](#).

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 приложения, полностью обновлены.

На серверах Kaspersky Private Security Network хранится конфиденциальная информация (например, журналы работы программы). Рекомендуется обеспечить дополнительную защиту серверов Kaspersky Private Security Network. После настройки дополнительной защиты убедитесь, что соединения, необходимые для работы приложения, доступны.

Некоторые параметры веб-плагина Kaspersky Private Security Network, используемые для взаимодействия с серверной частью Kaspersky Private Security Network, хранятся в хранилище Kaspersky Security Center. Хранилище доступно через Kaspersky Security Center OpenAPI™. Kaspersky Private Security Network не проводит контроль целостности хранилища данных плагина в Kaspersky Security Center. Администратору необходимо самостоятельно ограничить доступ к Kaspersky Security Center OpenAPI средствами Kaspersky Security Center, операционной системы или другими способами.

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

Однонаправленный шлюз требуется настроить так, чтобы он для каждого необходимого потока передавал файлы из директории `/var/kpsn/gateway_external/<имя потока>/data`, расположенной на сервере с компонентом Gateway External, в директорию `/var/kpsn/gateway_internal/<имя потока>`, расположенную на сервере с компонентом Gateway Internal, а затем удалял переданные файлы с сервера с компонентом Gateway External. Структуру вложенных директорий при передаче файлов следует сохранять, поэтому удалять нужно именно файлы, а не директории.

Передаваемые файлы должны иметь права 0666.

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

Установка серверной части Kaspersky Private Security Network

Серверная часть Kaspersky Private Security Network устанавливается с помощью скрипта установки `install.sh`.

Установку необходимо запускать на Управляющем узле кластера Kubernetes.

Чтобы установить серверную часть Kaspersky Private Security Network:

1. Распакуйте архив `KPSN_install_<версия>.tar.gz`.
2. Скачайте необходимое стороннее программное обеспечение с помощью команд:
 - Для Kaspersky Private Security Network 4.0–4.0.4:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```
 - Для Kaspersky Private Security Network 4.0.5 и выше:

```
cd ./images/  
sudo -E ./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

Вы можете скачать стороннее программное обеспечение на другой компьютер, а затем скопировать скачанные объекты в соответствующие папки распакованного архива.

3. Настройте использование кластером Kubernetes локального репозитория контейнеров:

a. Добавьте в файл `/etc/hosts` строку:

```
127.0.0.1 ksn-repo
```

b. Создайте файл `/etc/rancher/k3s/registries.yaml`, если он еще не существует. Добавьте в него следующие строки, соблюдая увеличение отступа на два пробела в начале каждой строки:

```
mirrors:
  "ksn-repo:31000":
    endpoint:
      - "http://ksn-repo:31000"
```

c. Перезапустите службу k3s с помощью команды:

```
sudo systemctl restart k3s.service
```

Шаг 3 необходимо выполнить на каждом сервере, входящем в кластер.

4. Перейдите в директорию с распакованным архивом `KPSN_install_<версия>.tar.gz` и запустите скрипт установки:

```
./install.sh
```

5. Ознакомьтесь с условиями Лицензионного соглашения, которое находится в указанной в ответе скрипта директории.

6. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку приложения и не должны использовать приложение.

7. Если вы согласны с условиями Лицензионного соглашения, запустите скрипт установки с параметром `--accept-eula`:

```
./install.sh --accept-eula
```

Скрипт установит компоненты, необходимые для работы Kaspersky Private Security Network, например пакеты Kubernetes. Дождитесь завершения работы скрипта.

Если вы устанавливаете Kaspersky Private Security Network версии 4.0.1 или выше, шаги 8-9 выполнять не нужно.

8. Скопируйте файл `kpsnctl` из архива в папку `/usr/local/bin` на сервере, на котором был выполнен предыдущий шаг, с помощью команды:

```
sudo cp ./kpsnctl /usr/local/bin
```

9. Укажите права для файла с помощью команды:

```
sudo chmod 755 /usr/local/bin/kpsnctl
```

Серверная часть Kaspersky Private Security Network будет установлена.

Получение файла интеграции с веб-плагином Kaspersky Private Security Network

После завершения установки серверной части Kaspersky Private Security Network нужно подготовить файл интеграции с веб-плагином Kaspersky Private Security Network. Файл интеграции включает в себя информацию, необходимую для организации соединения по протоколу TLS между серверной частью Kaspersky Private Security Network и веб-плагином Kaspersky Private Security Network. Для подготовки файла интеграции используется утилита kpsnctl. Утилита kpsnctl находится в установочном архиве серверной части Kaspersky Private Security Network.

Перед выполнением инструкции, приведенной ниже, получите CSR-файл в [мастере настройки веб-плагина Kaspersky Private Security Network](#) и скопируйте этот файл на сервер, где установлена серверная часть Kaspersky Private Security Network.

В командах ниже допускается указание нескольких имен. Если в используемый кластер Kubernetes входит несколько серверов, то в командах ниже для каждого сервера следует указать хотя бы одно имя. Параметр `--external-hostname` должен быть перед каждым именем.
Пример указания нескольких имен:
`kpsnctl certs rotate ca --external-hostname example1.com --external-hostname example2.com`

Чтобы подготовить файл интеграции с веб-плагином Kaspersky Private Security Network:

1. Сгенерируйте файлы сертификатов для Kaspersky Private Security Network:

- Если интеграция настраивается впервые, используйте следующую команду:
`kpsnctl certs rotate ca --external-hostname <имя хоста, доступное с сервера с установленным Kaspersky Security Center>`
- Если интеграция уже настраивалась ранее, используйте следующую команду:
`kpsnctl certs rotate server --external-hostname <имя хоста, доступное с сервера с установленным Kaspersky Security Center>`
- Если вы хотите провести ротацию удостоверяющего центра (англ. certificate authority, CA), который используется приложением Kaspersky Private Security Network, используйте следующую команду:
`kpsnctl certs rotate ca --force --external-hostname <имя хоста, доступное с сервера с установленным Kaspersky Security Center>`

При выполнении команды `kpsnctl certs rotate ca` ранее выписанные [сертификаты для API](#) становятся недействительными.

Если срок действия серверного сертификата истечет, возможны ошибки при использовании веб-плагина и API Kaspersky Private Security Network. Рекомендуется настроить регулярную ротацию серверного сертификата, например с помощью cron. Для настройки автоматической ротации раз в месяц выполните команду:

```
(crontab -l 2>/dev/null; echo "0 0 1 * * kpsnctl certs rotate server --external-hostname <имя хоста, доступное с сервера с установленным Kaspersky Security Center>") | crontab -
```

2. Сгенерируйте интеграционный файл:

```
kpsnctl generate-integration-file --client-csr <путь к CSR-файлу> --external-hostname <имя хоста, доступное с сервера с установленным Kaspersky Security Center> > integration.json
```

Полученный интеграционный файл integration.json нужен при настройке интеграции [в мастере настройки веб-плагина Kaspersky Private Security Network](#).

Установка веб-плагина Kaspersky Private Security Network

Установка веб-плагина на виртуальные серверы Kaspersky Security Center не поддерживается.

Веб-плагин Kaspersky Private Security Network устанавливается через веб-интерфейс Kaspersky Security Center Web Console.

Вам понадобятся следующие файлы из комплекта поставки:

- Установочный ZIP-архив с файлами веб-плагина.
- TXT-файл с подписью для проверки установочного ZIP-архива.

Чтобы запустить установку веб-плагина Kaspersky Private Security Network:

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Параметры консоли** → **Веб-плагины**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Параметры** → **Веб-плагины**.

2. Добавьте веб-плагин Kaspersky Private Security Network:

- a. Нажмите на кнопку **Добавить из файла**.
- b. По кнопке **Загрузить файл формата ZIP** загрузите ZIP-архив с файлами веб-плагина.
- c. По кнопке **Загрузить подпись** загрузите TXT-файл с подписью.
- d. Нажмите на кнопку **Добавить**.
- e. Перезагрузите страницу.

Веб-плагин Kaspersky Private Security Network должен появиться в списке веб-плагинов.

Если после установки веб-плагина разделы Kaspersky Private Security Network отсутствуют в веб-интерфейсе, перезапустите Kaspersky Security Center Web Console.

3. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

4. Нажмите на кнопку **Установить KPSN**.

Откроется мастер настройки Kaspersky Private Security Network. Далее описаны шаги мастера настройки.

Шаг 1. Интеграция серверной части Kaspersky Private Security Network и веб-плагина Kaspersky Private Security Network

Поддерживается интеграция серверной части только с одним веб-плагином одновременно.

На этом шаге выполняется подготовка к интеграции серверной части Kaspersky Private Security Network с веб-плагином Kaspersky Private Security Network.

Подготовка к интеграции включает в себя получение файла запроса на получение сертификата (CSR-файл), файла интеграции и проверку их соответствия друг другу.

Чтобы подготовить файлы, необходимые для интеграции:

1. В блоке **Запрос на подписание сертификата KPSN (CSR)** нажмите на кнопку **Загрузить** и получите CSR-файл.

При выполнении следующих действий не закрывайте и не обновляйте страницу мастера настройки, на которой вы получили CSR-файл.

2. На сервере, где установлена серверная часть Kaspersky Private Security Network, с помощью полученного CSR-файла [сгенерируйте интеграционный файл](#).
3. Вернитесь в мастер настройки Kaspersky Private Security Network.
4. По кнопке **Выбрать файл** загрузите интеграционный файл, полученный на сервере с установленной серверной частью Kaspersky Private Security Network.

Мастер настройки проверит, соответствует ли информация в файле данным о ранее полученном CSR-файле.

Если вы закрыли или перезагрузили страницу мастера настройки, данные в интеграционном файле будут некорректными. В этом случае нужно заново получить CSR-файл и соответствующий ему интеграционный файл.

При переходе к следующему шагу выполняется интеграция серверной части Kaspersky Private Security Network с веб-плагином Kaspersky Private Security Network. Интеграция может занимать несколько минут, дождитесь ее завершения.

Шаг 2. Загрузка активационного архива

На этом шаге вам необходимо предоставить активационный архив, полученный от "Лаборатории Касперского". По кнопке **Добавить файлы** загрузите этот архив в мастер настройки.

Мастер настройки проверит правильность данных в архиве. Если ошибок не обнаружено, вы можете перейти к следующему шагу.

Шаг 3. Выбор компонентов для установки

На этом шаге вы можете выбрать нужные вам серверные компоненты Kaspersky Private Security Network. В карточке каждого компонента можно выбрать количество экземпляров компонента, которые необходимо установить. Увеличение количества экземпляров приводит к увеличению производительности Kaspersky Private Security Network, но в то же время требует большего объема памяти и дискового пространства.

В зависимости от количества выбранных компонентов пересчитывается объем необходимого дискового пространства, информация об этом отображается в блоке **Требования**.

Шаг 4. Установка компонентов

На этом шаге вы можете проверить, какие компоненты и в каком количестве экземпляров подготовлены к установке.

Убедившись, что набор компонентов соответствует требуемому, нажмите на кнопку **Установить**.

Мастер настройки установит выбранные компоненты.

Шаг 5. Добавление ключей шифрования трафика

На этом шаге вы можете добавить один или несколько ключей шифрования трафика.

Ключи шифрования трафика необходимы для шифрования данных, передаваемых между сервисами Kaspersky Private Security Network и компьютерами с установленными приложениями "Лаборатории Касперского".

Добавить ключи шифрования трафика можно следующими способами:

- сгенерировать новый (кнопка **Создать ключ**);
- импортировать существующий (кнопка **Загрузить ключ**).

Шаг 6. Добавление идентификатора установки

На этом шаге указываются данные, с помощью которых можно идентифицировать установленный Kaspersky Private Security Network:

- В поле **Имя установки KPSN** введите произвольное имя. Это обязательный параметр.

Имя установки – ваш уникальный идентификатор для "Лаборатории Касперского". Оно будет использоваться при получении обновлений и сертификатов.

Не используйте тестовое название, потому что имя установки невозможно изменить в дальнейшем. Введенное здесь значение будет использоваться для будущих обновлений.

- В полях ниже вы можете ввести адреса, по которым Kaspersky Private Security Network будет доступен для других приложений \ "Лаборатории Касперского\".

- В поле **Адреса для внутреннего доступа** укажите IP-адрес или URL для доступа внутри сети, в которой установлен сервер KPSN

- В поле **Адреса для внешнего доступа** укажите IP-адрес или URL для доступа из внешней сети.

Поддерживается только формат адреса IPv4.

Шаг 7. Проверка конфигурации

На этом шаге вы можете проверить параметры устанавливаемого Kaspersky Private Security Network.

Завершение установки

По завершении установки нажмите на кнопку **Завершить установку и запустить KPSN**.

Обновление Kaspersky Private Security Network

Обновление Kaspersky Private Security Network до версии 4.0.1 и выше доступно для Kaspersky Private Security Network версий 4.0 выше. Обновления каждой версии являются кумулятивными: например, для обновления серверной части Kaspersky Private Security Network 4.0 до версии 4.0.3 достаточно установить версию 4.0.3, пропустив установку версий 4.0.1 и 4.0.2.

Обновление может включать в себя один из следующих шагов или сразу оба:

- [Обновление веб-плагина Kaspersky Private Security Network](#).
- [Обновление серверной части Kaspersky Private Security Network](#).

Если обновление предполагает и обновление серверной части, и обновление веб-плагина, необходимо сначала установить обновление веб-плагина, а затем обновление серверной части Kaspersky Private Security Network.

Вы можете просмотреть версию используемого веб-плагина Kaspersky Private Security Network в веб-интерфейсе Kaspersky Security Center Web Console в разделе **KPSN** → **Параметры** → **Веб-плагины** (в Kaspersky Security Center Web Console 14.2 – в разделе **Параметры консоли** → **Веб-плагины**).

Вы можете просмотреть версию используемой серверной части Kaspersky Private Security Network в веб-интерфейсе Kaspersky Security Center Web Console в разделе **KPSN** → **Параметры** → **О KPSN** (в Kaspersky Security Center Web Console 14.2 – в разделе **Операции** → **Параметры KPSN** → **О KPSN**).

Обновление веб-плагина Kaspersky Private Security Network

Обновление веб-плагина Kaspersky Private Security Network устанавливается через веб-интерфейс Kaspersky Security Center Web Console.

Вам понадобятся следующие файлы:

- Установочный ZIP-архив с файлами обновления веб-плагина.
- TXT-файл с подписью для проверки установочного ZIP-архива.

Чтобы установить обновление веб-плагина Kaspersky Private Security Network:

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Параметры консоли** → **Веб-плагины**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Параметры** → **Веб-плагины**.

2. Добавьте веб-плагин Kaspersky Private Security Network:

- a. Нажмите на кнопку **Обновить из файла**, чтобы загрузить обновление для веб-плагина из файла.
- b. Укажите файл и подпись файла.
- c. Загрузите указанный файл.

Веб-плагин Kaspersky Private Security Network будет обновлен из файла и появится в списке веб-плагинов управления Kaspersky Security Center Web Console.

Обновление серверной части Kaspersky Private Security Network

Серверная часть Kaspersky Private Security Network обновляется с помощью скрипта установки `install.sh`.

Обновление необходимо запускать на Управляющем узле кластера Kubernetes. Если таких узлов несколько, рекомендуется выбрать узел, на котором выполнялась установка Kaspersky Private Security Network.

Чтобы обновить серверную часть Kaspersky Private Security Network:

1. Убедитесь, что выполняются [требования к программному и аппаратному обеспечению](#).
2. Распакуйте архив `KPSN_install_<версия>.tar.gz`.
3. Скачайте необходимое стороннее программное обеспечение с помощью команд:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

Вы можете скачать стороннее программное обеспечение на другой компьютер, а затем скопировать скачанные объекты в соответствующие папки распакованного архива.

4. Перейдите в директорию с распакованным архивом `KPSN_install_<версия>.tar.gz` и запустите скрипт:
`./install.sh`
5. Если скрипт сообщит о необходимости принятия Лицензионного соглашения для установки обновления, выполните следующие действия:
 - a. Ознакомьтесь с условиями Лицензионного соглашения, которое находится в указанной в ответе скрипта директории.
 - b. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку приложения и не должны использовать приложение.

с. Если вы согласны с условиями Лицензионного соглашения, запустите скрипт установки с параметром --accept-eula:

```
./install.sh --accept-eula
```

Скрипт установит обновление Kaspersky Private Security Network.

Установка обновления не влияет на настроенные параметры работы и базы данных Kaspersky Private Security Network.

Обновление Kaspersky Private Security Network до версии 4.0.1

Обновление Kaspersky Private Security Network до версии 4.0.1 доступно только с версии Kaspersky Private Security Network 4.0.

Обновление Kaspersky Private Security Network до версии 4.0.1 включает следующие этапы:

- 1 [Обновление веб-плагина Kaspersky Private Security Network](#)
- 2 [Обновление серверной части Kaspersky Private Security Network](#)

После обновления будет использоваться веб-плагин Kaspersky Private Security Network версии 1.1.0.33, серверная часть Kaspersky Private Security Network версии 4.0.375.

Обновление Kaspersky Private Security Network до версии 4.0.2

Обновление Kaspersky Private Security Network до версии 4.0.2 доступно с Kaspersky Private Security Network версий 4.0 и 4.0.1.

Обновление Kaspersky Private Security Network с версии 4.0 до версии 4.0.2 включает следующие этапы:

- 1 [Обновление веб-плагина Kaspersky Private Security Network](#)
- 2 [Обновление серверной части Kaspersky Private Security Network](#)

Для обновления Kaspersky Private Security Network с версии 4.0.1 до версии 4.0.2 необходимо [обновить серверную часть Kaspersky Private Security Network](#), обновление веб-плагина не требуется.

После обновления будет использоваться веб-плагин Kaspersky Private Security Network версии 1.1.0.33, серверная часть Kaspersky Private Security Network версии 4.0.430.

Обновление Kaspersky Private Security Network до версии 4.0.3

Обновление Kaspersky Private Security Network до версии 4.0.3 доступно с Kaspersky Private Security Network версии 4.0 и выше.

Чтобы обновить Kaspersky Private Security Network до версии 4.0.3:

1. Убедитесь, что версия используемого веб-плагина Kaspersky Private Security Network – 1.1.0.33 (соответствует версии 4.0.1). Для этого выполните одно из следующих действий:
 - В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Параметры консоли** → **Веб-плагины**.
 - В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Параметры** → **Веб-плагины**.
2. Если версия веб-плагина отличается, установите [обновление веб-плагина](#) для версии 4.0.1.
3. [Обновите серверную часть Kaspersky Private Security Network](#).

Приложение Kaspersky Private Security Network будет обновлено до версии 4.0.3. После обновления будет использоваться серверная часть Kaspersky Private Security Network версии 4.0.527.

Обновление Kaspersky Private Security Network до версии 4.0.4

Обновление Kaspersky Private Security Network до версии 4.0.4 доступно с Kaspersky Private Security Network версии 4.0 и выше.

Чтобы обновить Kaspersky Private Security Network до версии 4.0.4:

1. Убедитесь, что версия используемого веб-плагина Kaspersky Private Security Network – 1.1.0.33 (соответствует версии 4.0.1). Для этого выполните одно из следующих действий:
 - В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Параметры консоли** → **Веб-плагины**.
 - В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Параметры** → **Веб-плагины**.
2. Если версия веб-плагина отличается, установите [обновление веб-плагина](#) для версии 4.0.1.
3. Обновите серверную часть Kaspersky Private Security Network:
 - a. Убедитесь, что выполняются [требования к программному и аппаратному обеспечению](#).
 - b. Распакуйте архив KPSN_install_<версия>.tar.gz.

с. Скачайте необходимое стороннее программное обеспечение с помощью команд:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

Вы можете скачать стороннее программное обеспечение на другой компьютер, а затем скопировать скачанные объекты в соответствующие папки распакованного архива.

d. Перейдите в директорию с распакованным архивом KPSN_install_<версия>.tar.gz и запустите скрипт:

```
./upgrade.sh
```

e. Если скрипт сообщит о необходимости принятия Лицензионного соглашения для установки обновления, выполните следующие действия:

1. Ознакомьтесь с условиями Лицензионного соглашения, которое находится в указанной в ответе скрипта директории.
2. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать обновление и не должны использовать приложение.
3. Если вы согласны с условиями Лицензионного соглашения, запустите скрипт обновления с параметром `--accept-eula`:

```
./upgrade.sh --accept-eula
```

Приложение Kaspersky Private Security Network будет обновлено до версии 4.0.4.

Установка обновления не влияет на настроенные параметры работы и базы данных Kaspersky Private Security Network.

Обновление Kaspersky Private Security Network до версии 4.0.5

Обновление Kaspersky Private Security Network до версии 4.0.5 доступно с Kaspersky Private Security Network версии 4.0 и выше.

Перед обновлением серверной части рекомендуется **сохранить локальные репутационные базы**.

Чтобы экспортировать данные из локальной репутационной базы:

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Репутационные списки KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Репутационные списки**.

- Если вы хотите экспортировать сведения о репутации файлов, выберите вкладку **File Reputation**.
- Если вы хотите экспортировать сведения о репутации веб-сайтов, выберите вкладку **URL Reputation**.

2. Нажмите на кнопку **Экспорт списка**:

- 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. В список будут включены все добавленные в локальную базу и не удаленные ранее объекты.

Чтобы обновить Kaspersky Private Security Network до версии 4.0.5:

1. Убедитесь, что версия используемого веб-плагина Kaspersky Private Security Network – 1.1.0.33 (соответствует версии 4.0.1). Для этого выполните одно из следующих действий:

- В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Параметры консоли** → **Веб-плагины**.
- В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Параметры** → **Веб-плагины**.

2. Если версия веб-плагина отличается, установите [обновление веб-плагина](#) для версии 4.0.1.

3. Обновите серверную часть Kaspersky Private Security Network:

a. Убедитесь, что выполняются [требования к программному и аппаратному обеспечению](#).

b. Распакуйте архив KPSN_install_<версия>.tar.gz.

c. Скачайте необходимое стороннее программное обеспечение с помощью команд:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

Вы можете скачать стороннее программное обеспечение на другой компьютер, а затем скопировать скачанные объекты в соответствующие папки распакованного архива.

d. Перейдите в директорию с распакованным архивом KPSN_install_<версия>.tar.gz и запустите скрипт:

```
./install.sh
```

е. Если скрипт сообщит о необходимости принятия Лицензионного соглашения для установки обновления, выполните следующие действия:

1. Ознакомьтесь с условиями Лицензионного соглашения, которое находится в указанной в ответе скрипта директории.
2. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать обновление и не должны использовать приложение.
3. Если вы согласны с условиями Лицензионного соглашения, запустите скрипт обновления с параметром `--accept-eula`:

```
./install.sh --accept-eula
```

Приложение Kaspersky Private Security Network будет обновлено до версии 4.0.5.

Установка обновления не влияет на настроенные параметры работы и базы данных Kaspersky Private Security Network.

Обновление Kaspersky Private Security Network до версии 4.0.6

Обновление Kaspersky Private Security Network до версии 4.0.6 доступно с Kaspersky Private Security Network версии 4.0 и выше.

Перед обновлением серверной части рекомендуется **сохранить локальные репутационные базы**.

Чтобы экспортировать данные из локальной репутационной базы:

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Репутационные списки KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Репутационные списки**.

- Если вы хотите экспортировать сведения о репутации файлов, выберите вкладку **File Reputation**.
- Если вы хотите экспортировать сведения о репутации веб-сайтов, выберите вкладку **URL Reputation**.

2. Нажмите на кнопку **Экспорт списка**:

- 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. В список будут включены все добавленные в локальную базу и не удаленные ранее объекты.

Чтобы обновить Kaspersky Private Security Network до версии 4.0.6:

1. Убедитесь, что версия используемого веб-плагина Kaspersky Private Security Network – 1.1.0.33 (соответствует версии 4.0.1). Для этого выполните одно из следующих действий:

- В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Параметры консоли** → **Веб-плагины**.
- В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Параметры** → **Веб-плагины**.

2. Если версия веб-плагина отличается, установите [обновление веб-плагина](#) для версии 4.0.1.

3. Удалите [интеграцию с веб-плагином Kaspersky Private Security Network](#).

4. Обновите серверную часть Kaspersky Private Security Network:

a. Убедитесь, что выполняются [требования к программному и аппаратному обеспечению](#).

b. Распакуйте архив KPSN_install_<версия>.tar.gz.

c. Скачайте необходимое стороннее программное обеспечение с помощью команд:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

Вы можете скачать стороннее программное обеспечение на другой компьютер, а затем скопировать скачанные объекты в соответствующие папки распакованного архива.

d. Перейдите в директорию с распакованным архивом KPSN_install_<версия>.tar.gz и запустите скрипт:

```
./install.sh
```

e. Если скрипт сообщит о необходимости принятия Лицензионного соглашения для установки обновления, выполните следующие действия:

1. Ознакомьтесь с условиями Лицензионного соглашения, которое находится в указанной в ответе скрипта директории.
2. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать обновление и не должны использовать приложение.
3. Если вы согласны с условиями Лицензионного соглашения, запустите скрипт обновления с параметром `--accept-eula`:

```
./install.sh --accept-eula
```

5. Если при обновлении серверной части Kaspersky Private Security Network возникли проблемы, например отсутствие прогресса обновления, выполните следующие действия:

- a. В кластере в пространстве имен kpsn найдите поды в состоянии *Error* с помощью команды:
- ```
kubectl -n kpsn get pods | grep -i error
```

b. Удалите найденные поды с помощью команды:

```
kubectl -n kpsn delete pod < имя_пода1 > < имя_пода2 >
```

с. Повторно запустите скрипт обновления серверной части (п. 4d).

6. Выполните интеграцию серверной части Kaspersky Private Security Network и веб-плагина Kaspersky Private Security Network.

Приложение Kaspersky Private Security Network будет обновлено до версии 4.0.6.

Установка обновления не влияет на настроенные параметры работы и базы данных Kaspersky Private Security Network.

# Удаление интеграции с Kaspersky Private Security Network

Вы можете удалить интеграцию с Kaspersky Private Security Network на текущем Сервере администрирования.

Удаление интеграции может быть полезно в следующих случаях:

- Если вы хотите перенести управление Kaspersky Private Security Network на другой сервер Kaspersky Security Center Web Console.
- Если вы хотите прекратить использование веб-плагина или удалить веб-плагин.  
При удалении веб-плагина рекомендуется сначала удалить интеграцию с веб-плагином. Удаление веб-плагина выполняется средствами Kaspersky Security Center Web Console. Более подробную информацию см. в *справке Kaspersky Security Center Web Console*.
- Если в работе Kaspersky Private Security Network возникли ошибки.

Чтобы удалить интеграцию веб-плагина и серверной части Kaspersky Private Security Network:

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

2. На вкладке **Параметры** в блоке **Удаление интеграции с KPSN** нажмите на кнопку **Удалить интеграцию с сервером KPSN**.
3. В открывшемся окне подтвердите действие.

Интеграция с Kaspersky Private Security Network на текущем Сервере администрирования будет удалена.

После удаления интеграции веб-плагин Kaspersky Private Security Network вернется в исходное состояние. Данные серверной части и сервисов Kaspersky Private Security Network не будут затронуты, сервисы Kaspersky Private Security Network продолжат работу. Вы можете использовать серверную часть Kaspersky Private Security Network на другом сервере Kaspersky Security Center, повторив [интеграцию](#).

# Удаление Kaspersky Private Security Network

Удаление Kaspersky Private Security Network состоит из следующих этапов:

1. Удаление серверной части Kaspersky Private Security Network.

Серверная часть удаляется с помощью запуска скрипта `./uninstall.sh` из установочного архива серверной части Kaspersky Private Security Network.

2. Удаление веб-плагина.

При удалении веб-плагина рекомендуется сначала удалить интеграцию с веб-плагином. Удаление веб-плагина выполняется средствами Kaspersky Security Center Web Console. Более подробную информацию см. в *справке Kaspersky Security Center Web Console*.

# Сертификат для получения обновлений

Сертификат для обновлений требуется для того, чтобы компоненты Kaspersky Private Security Network могли взаимодействовать с серверами "Лаборатории Касперского":

- [Получать обновления баз данных.](#)
- [Получать конфигурационные файлы.](#)

Сертификат загружается в Kaspersky Private Security Network в составе активационного архива при [настройке Kaspersky Private Security Network](#). Информация о состоянии и сроке годности сертификата для получения обновлений отображается в следующих разделах:

- В веб-интерфейсе Kaspersky Security Center Web Console 14.2: в разделе **Операции** → **Параметры KPSN** → **Конфигурация**.
- В веб-интерфейсе Kaspersky Security Center Web Console другой версии: в разделе **Программы и службы** → **KPSN** → **Параметры** → **Конфигурация**.

Для получения нового сертификата обновления вам нужно отправить запрос в Службу технической поддержки "Лаборатории Касперского". Полученный архив, содержащий сертификат, следует импортировать в Kaspersky Private Security Network.

*Чтобы импортировать архив, содержащий сертификат для получения обновлений, в Kaspersky Private Security Network:*

1. Обратитесь в [Службу поддержки](#) с запросом нового сертификата для получения обновлений Kaspersky Private Security Network.
2. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.
3. На вкладке **Конфигурация KPSN** нажмите на **Сертификат**.  
Откроется окно с информацией о текущем сертификате.
4. Нажмите на кнопку **Импортировать новый сертификат**.
5. В открывшемся окне нажмите на кнопку **Обзор** и выберите архив, полученный от "Лаборатории Касперского".
6. Нажмите на кнопку **Сохранить**.

Новый сертификат будет импортирован в Kaspersky Private Security Network.

# Обновление баз

Kaspersky Private Security Network получает обновления баз по протоколу HTTPS с использованием шифрованного канала связи.

## Обновление баз для простой конфигурации

Для простой конфигурации Kaspersky Private Security Network обновление баз выполняется по следующему алгоритму:

1. Сервис Kaspersky Private Security Network на стороне локальной сети вашей организации отправляет запрос на получение обновлений на сервер "Лаборатории Касперского".
2. Сервер "Лаборатории Касперского" на основе данных из запроса определяет наличие обновлений.
3. Сервер "Лаборатории Касперского" отправляет на серверы с сервисами Kaspersky Private Security Network ответ с обновлениями баз.

Этот алгоритм повторяется для всех потоков обновления, необходимых установленным сервисам Kaspersky Private Security Network:

## Обновление баз для конфигурации с использованием прокси-сервера

В конфигурации с использованием прокси-сервера Kaspersky Private Security Network отправляет запросы и получает ответы на них через [указанный администратором прокси-сервер](#).

## Обновление баз для конфигурации с использованием однонаправленного шлюза

В конфигурации с использованием однонаправленного шлюза обновление баз состоит из процессов, повторяющихся в цикле.

Компонент Gateway External получает обновления баз в открытом сегменте сети по следующему алгоритму:

1. Gateway External в открытом сегменте локальной сети вашей организации отправляет на сервер "Лаборатории Касперского" запрос на получение обновлений.
2. Сервер "Лаборатории Касперского" на основе данных из запроса определяет наличие обновлений.
3. Сервер "Лаборатории Касперского" отправляет на сервер с Gateway External ответ с обновлениями баз.
4. Gateway External записывает полученные обновления в файл.

Для Kaspersky Private Security Network с однонаправленным шлюзом потоки обновлений дополнительно упаковываются в файлы для обмена между компонентами Gateway External и Gateway Internal. Передача обновлений баз между открытым и категоризованным сегментами сети происходит по следующему алгоритму:

1. Однонаправленный шлюз, используемый в организации, перемещает файлы в категоризованный сегмент в папку, используемую Gateway External.
2. Gateway Internal записывает обновления из файла во внутренний поток обновления.
3. Сервис Kaspersky Private Security Network в категоризованном сегменте получает обновления из внутреннего потока.

В Kaspersky Private Security Network версии 4.0.1 и выше на вкладке **Конфигурация** в карточках компонентов Gateway Internal и Gateway External указан сервер, на котором развёрнут соответствующий компонент. Папки, используемые компонентом, находятся на указанном сервере.

Обновление баз сервисов в категоризованном сегменте происходит по следующему алгоритму:

1. Сервис Kaspersky Private Security Network на стороне локальной сети вашей организации отправляет запрос на получение обновлений на сервер с компонентом Gateway Internal.
2. Сервер с компонентом Gateway Internal на основе данных из запроса определяет наличие обновлений.
3. Сервер с компонентом Gateway Internal отправляет на серверы с сервисами Kaspersky Private Security Network ответ с обновлениями баз.

## Запрос на обновление баз

Для обновления баз компоненты Kaspersky Private Security Network отправляют 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, созданный при установке серверной части Kaspersky Private Security Network;
- идентификатор сервиса Kaspersky Private Security Network;
- имя потока обновлений баз;
- дата последнего обновления баз;
- идентификатор запрашиваемого сообщения обновления;

- количество запрашиваемых сообщений обновления;
- максимальное время ожидания ответа.

## Контроль обновления баз

Вы можете контролировать обновление баз Kaspersky Private 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. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 выберите раздел **Мониторинг и отчеты** → **Журнал обновлений баз KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии выберите раздел **Программы и службы** → **KPSN** → **Журнал обновлений баз**.

2. Нажмите на кнопку **Обновить**, чтобы актуализировать данные.

Отобразится таблица с потоками данных, которые были обновлены в Kaspersky Private Security Network.

## Устранение сбоев передачи данных через однонаправленный шлюз

Во время загрузки пакетов с репутационными базами из открытого сегмента сети в категоризированный сегмент сети через однонаправленный шлюз может произойти сбой. Об ошибке вы можете узнать в веб-интерфейсе категоризированного сегмента сети Kaspersky Private Security Network. При возникновении ошибки в веб-интерфейсе категоризированного сегмента сети в разделе **Параметры KPSN** на вкладке **Конфигурация** в статусе компонента Gateway Internal отображается значок .

*Чтобы устранить ошибку загрузки обновлений баз:*

1. Откройте веб-интерфейс категоризированного сегмента сети Kaspersky Private Security Network.

2. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

3. На вкладке **Конфигурация** нажмите на компонент **Gateway Internal**.

Откроется окно **Статусы потоков данных**. Потоки данных, во время загрузки которых произошла ошибка, будут выделены 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.

6. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

7. На вкладке **Конфигурация** нажмите на компонент **Gateway External**.

Откроется окно **Обновление потока данных**.

8. В раскрывающемся списке **Поток** выберите поток, при загрузке данных которого произошла ошибка.

9. В поле **Код статуса** введите код этого потока обновлений, полученный в п. 4.

10. Нажмите на кнопку **Обновить**.

Загрузка потока обновления продолжится с сообщения, соответствующего введённому значению.

11. Повторите действия пунктов 8-10 для всех потоков обновления данных, во время загрузки которых произошла ошибка.

# Настройка прокси-сервера

Вы можете настроить использование прокси-сервера для взаимодействия компонентов Kaspersky Private Security Network с серверами "Лаборатории Касперского".

Компоненты Kaspersky Private Security Network взаимодействуют с серверами "Лаборатории Касперского" в следующих случаях:

- При получении [обновлений баз](#).
- При запросе [конфигурационных файлов через веб-плагин](#).

*Чтобы настроить прокси-сервер:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

2. На вкладке **Параметры** в блоке **Прокси-сервер** нажмите на кнопку **Настроить подключение**.

3. В открывшемся окне настройте параметры подключения к прокси-серверу:

- a. Если вы хотите использовать прокси-сервер, включите переключатель **Использовать прокси-сервер**.

Настройка параметров прокси-сервера недоступна, если переключатель выключен.

- b. В поле **Адрес прокси-сервера** укажите адрес в формате имени DNS-сервера или адреса IPv4.

- c. В поле **Порт** укажите порт прокси-сервера.

- d. В раскрывающемся списке **Аутентификация** выберите тип аутентификации.

Возможные значения: **Без аутентификации**, **По логину и паролю**.

- e. Если вы выбрали аутентификацию по логину и паролю, в полях **Логин** и **Пароль** ведите учетные данные для аутентификации.

- f. Нажмите на кнопку **Проверить соединение** для проверки возможности подключения к прокси-серверу.

- g. Если введенные параметры корректны, нажмите на кнопку **Сохранить**.

Соединение с прокси-сервером будет настроено.

# Конфигурация Kaspersky Private Security Network

Конфигурация Kaspersky Private Security Network определяется при настройке Kaspersky Private Security Network. Конфигурация включает в себя:

- Имя установки.

Задается только при [настройке](#).

- Компоненты Kaspersky Private Security Network.

Компоненты устанавливаются при [настройке Kaspersky Private Security Network](#). Вы можете [просмотреть информацию о составе и количестве установленных компонентов](#) и при необходимости [добавить или удалить компоненты](#).

- [Внутренние и внешние адреса доступа к Kaspersky Private Security Network](#).

- Открытые ключи шифрования трафика.

Ключи шифрования трафика добавляются при [настройке Kaspersky Private Security Network](#). Вы можете просмотреть информацию о текущих ключах шифрования трафика или [добавить новые ключи шифрования](#).

При изменении конфигурации Kaspersky Private Security Network следует [получить новый конфигурационный файл](#) и передать его в приложения, которые используют Kaspersky Private Security Network.

## Просмотр информации о конфигурации

*Чтобы просмотреть информацию о составе конфигурации Kaspersky Private Security Network,*

в веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**,

в веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

На вкладке **Конфигурация** отображается следующая информация:

- Имя установки Kaspersky Private Security Network.

- Установленные компоненты и их количество.

Для просмотра информации о компоненте вы можете нажать на компонент.

- [Состояние и срок действия сертификата для получения обновлений Kaspersky Private Security Network](#).

- Состояние и срок действия [ключей шифрования трафика](#).

Для просмотра информации о текущих ключах шифрования трафика вы можете нажать на **Ключи шифрования трафика**.

# Добавление и удаление компонентов

Чтобы добавить или удалить компоненты Kaspersky Private Security Network:

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.
2. На вкладке **Конфигурация** нажмите на компонент, количество экземпляров которого вы хотите изменить.  
Откроется окно с информацией о компоненте.
3. В поле **Количество** укажите количество экземпляров компонента, которое вам нужно. Для удаления компонента установите значение 0.

Для добавления компонентов требуется дополнительное место на сервере.

4. Нажмите на кнопку **Сохранить**.
5. Подтвердите добавление или удаление компонента в окне подтверждения.

Компонент Kaspersky Private Security Network будет установлен или удален.

Информация об установленных компонентах отобразится на вкладке **Конфигурация**.

## Получение конфигурационных файлов Kaspersky Private Security Network

Для того чтобы приложения "Лаборатории Касперского" могли использовать Kaspersky Private Security Network, вам необходимо получить архив с параметрами подключения к серверам службы Kaspersky Private Security Network и импортировать его в приложения "Лаборатории Касперского".

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

Подробнее о настройке использования Kaspersky Private Security Network другими приложениями "Лаборатории Касперского" см. в документации к этим приложениям.

Архив с новыми конфигурационными файлами следует формировать после каждого изменения конфигурации Kaspersky Private Security Network и затем передавать его в приложения "Лаборатории Касперского", использующие Kaspersky Private Security Network.

Способ получения архива с конфигурационными файлами отличается в зависимости от [схемы развертывания Kaspersky Private Security Network](#) и расположения экземпляра Kaspersky Private Security Network, конфигурация которого была изменена, в этой схеме.

## Стандартная конфигурация и конфигурация с прокси-сервером

*Чтобы получить конфигурационные файлы для текущего экземпляра Kaspersky Private Security Network:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.
2. На вкладке **Конфигурация** нажмите на кнопку **Скачать конфигурационные файлы этого экземпляра KPSN**.

На ваш компьютер будет загружен архив с конфигурационными файлами.

## Конфигурация с однонаправленным шлюзом

*Чтобы получить конфигурационные файлы для Kaspersky Private Security Network в категоризованном сегменте сети:*

1. В веб-интерфейсе приложения Kaspersky Security Center Web Console 14.2, установленного в категоризованном сегменте сети, перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе приложения Kaspersky Security Center Web Console другой версии, установленного в категоризованном сегменте сети, перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.
2. На вкладке **Конфигурация** нажмите на кнопку **Экспортировать конфигурацию**.
3. В открывшемся окне нажмите на кнопку **Экспорт**.  
На ваш компьютер будет загружен файл configuration.json.
4. В веб-интерфейсе приложения Kaspersky Security Center Web Console 14.2, установленного в открытом сегменте сети, перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе приложения Kaspersky Security Center Web Console другой версии, установленного в открытом сегменте сети, перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.
5. На вкладке **Конфигурация** нажмите на кнопку **Получить конфигурационные файлы для KPSN за шлюзом**.
6. В открывшемся окне выберите файл configuration.json, полученный в п. 2.
7. Нажмите на кнопку **Получить файлы**.

На ваш компьютер будет загружен архив с конфигурационными файлами.

*Чтобы получить конфигурационные файлы для Kaspersky Private Security Network в открытом сегменте сети:*

1. В веб-интерфейсе приложения Kaspersky Security Center Web Console 14.2, установленного в открытом сегменте сети, перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе приложения Kaspersky Security Center Web Console другой версии, установленного в открытом сегменте сети, перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.
2. На вкладке **Конфигурация** нажмите на кнопку **Скачать конфигурационные файлы этого экземпляра KPSN**.

На ваш компьютер будет загружен архив с конфигурационными файлами.

## Экспорт конфигурации при ошибке получения конфигурационных файлов

Если вам не удалось получить конфигурационные файлы указанными выше способами, вы можете экспортировать конфигурацию Kaspersky Private Security Network и прислать полученный файл в Службу технической поддержки "Лаборатории Касперского".

*Чтобы экспортировать конфигурацию:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.
2. На вкладке **Конфигурация** нажмите на кнопку **Экспортировать конфигурацию**.
3. В открывшемся окне нажмите на кнопку **Экспорт**.

На ваш компьютер будет загружен файл configuration.json.

В запрос на получение конфигурационного файла включаются следующие сведения:

- идентификатор установки Kaspersky Private Security Network, сгенерированный при установке;
- версия Kaspersky Private Security Network;
- заданные внутренние и внешние адреса Kaspersky Private Security Network;
- идентификаторы установленных компонентов Kaspersky Private Security Network;
- открытые ключи шифрования трафика между Kaspersky Private Security Network и приложениями, использующими Kaspersky Private Security Network, и информация об их сроках действия.

Вам нужно отправить конфигурационный файл в "Лабораторию Касперского". В ответном сообщении вы получите конфигурационные файлы для настройки Kaspersky Private Security Network в других приложениях "Лаборатории Касперского".

# Шифрование трафика

Данные, передаваемые между серверами Kaspersky Private Security Network, Kaspersky Security Network и компьютерами с установленными приложениями "Лаборатории Касперского", должны быть зашифрованы. Для шифрования используются ключи шифрования трафика.

Вы можете просмотреть информацию о состоянии и сроке годности ключей шифрования трафика:

- Для просмотра информации о ключе для шифрования соединения между серверами Kaspersky Private Security Network и компьютерами с установленными приложениями "Лаборатории Касперского" перейдите в раздел **Операции** → **Параметры KPSN** → **Конфигурация** → **Ключи шифрования трафика**.
- Срок действия ключа для шифрования соединения между серверами Kaspersky Private Security Network и Kaspersky Security Network совпадает со сроком действия сертификата для получения обновлений. Для просмотра срока действия сертификата для получения обновлений перейдите в раздел **Операции** → **Параметры KPSN** → **Конфигурация** → **Сертификат**.

Трафик между серверами Kaspersky Private Security Network и компьютерами с установленными приложениями "Лаборатории Касперского"

Обеспечение шифрования трафика состоит из следующих этапов:

## 1 Добавление ключа шифрования трафика для безопасного обмена данными между серверами Kaspersky Private Security Network и компьютерами организации

В Kaspersky Private Security Network ключи шифрования находятся в хранилище ключей шифрования. Ключ шифрования трафика имеет срок действия 1000 дней.

Вы можете добавить ключи следующими способами:

- [Создание ключа](#). Добавление ключа выполняется автоматически.
- [Добавление существующего ключа](#), созданного сторонним программным обеспечением (например, с помощью пакета OpenSSL).
- [Импорт ранее экспортированного хранилища](#).

## 2 [Получение конфигурационных файлов для приложений "Лаборатории Касперского"](#)

Конфигурационные файлы с параметрами подключения к серверам службы Kaspersky Private Security Network содержат открытые ключи шифрования.

## 3 Добавление конфигурационных файлов в приложения "Лаборатории Касперского"

Подробнее о настройке использования Kaspersky Private Security Network другими приложениями "Лаборатории Касперского" см. в документации к этим приложениям.

Закрытые ключи шифрования можно получить с сервера Kaspersky Private Security Network при экспорте хранилища ключей.

Трафик между серверами Kaspersky Private Security Network и Kaspersky Security Network

Шифрование трафика обеспечивается [загрузкой активационного архива](#).

## Создание ключа шифрования трафика

*Чтобы создать ключ шифрования трафика:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.
2. На вкладке **Конфигурация** нажмите на **Ключи шифрования трафика**.
3. В открывшемся окне нажмите на кнопку **Создать ключ**.

Ключ шифрования трафика будет создан и автоматически добавлен в Kaspersky Private Security Network.

## Добавление ключа шифрования трафика

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 приложения.

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. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

2. На вкладке **Конфигурация** нажмите на **Ключи шифрования трафика**.
3. В открывшемся окне нажмите на кнопку **Загрузить ключ**.
4. Выберите файл закрытого ключа.
5. Нажмите на кнопку **Открыть**.

Ключ шифрования трафика будет добавлен в Kaspersky Private Security Network.

## Экспорт и импорт хранилища ключей шифрования трафика

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

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

2. На вкладке **Конфигурация** нажмите на **Ключи шифрования трафика**.
3. В открывшемся окне нажмите на кнопку **Экспорт ключей**.

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

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

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

2. На вкладке **Конфигурация** нажмите на **Ключи шифрования трафика**.
3. В открывшемся окне нажмите на кнопку **Импорт ключей** и в открывшемся окне выберите DAT-файл хранилища ключей.

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

4. Нажмите на кнопку **Открыть**.

Хранилище ключей шифрования трафика будет загружено в Kaspersky Private Security Network. Ключи будут удалены и заменены ключами из загруженного DAT-файла.

# Адреса доступа к сервисам Kaspersky Private Security Network

Адреса доступа к сервисам Kaspersky Private Security Network – это внутренние и внешние IP-адреса или имена узлов, по которым сервисы Kaspersky Private Security Network доступны для других приложений "Лаборатории Касперского". Адреса для внутреннего доступа должны принадлежать той же сети, в которой установлен сервер KPSN. Адреса для внешнего доступа – это адреса за пределами этой сети.

Адреса доступа входят в состав конфигурации Kaspersky Private Security Network. При изменении адресов доступа следует [получить новый конфигурационный файл](#) и передать его в приложения, которые используют Kaspersky Private Security Network.

Если адреса доступа были заданы при [настройке](#), вы можете просмотреть адреса в разделе **Параметры KPSN** на вкладке **Параметры** в блоке **Адреса доступа KPSN**.

*Чтобы указать адреса доступа к Kaspersky Private Security Network:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

2. На вкладке **Параметры** в блоке **Адреса доступа KPSN** нажмите на кнопку **Указать адреса**.

3. В открывшемся окне укажите адреса доступа:

- a. Если вы хотите указать внутренний адрес доступа, на вкладке **Внутренний доступ** нажмите на кнопку **Добавить** и введите IP-адрес или имя узла.
- b. Если вы хотите указать внешний адрес доступа, на вкладке **Внешний доступ** нажмите на кнопку **Добавить** и введите IP-адрес или имя узла.

При необходимости повторите добавление для нужного количества адресов. Для удаления адреса из списка нажмите на значок **x** справа от адреса.

4. Нажмите на кнопку **Сохранить**.

Адреса доступа будут указаны.

# 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](#). Данные локальных репутационных баз доступны только для компьютеров организации.

Репутация объекта в локальной репутационной базе имеет более высокий приоритет, чем репутация в Kaspersky Security Network. Например, 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 осуществляться 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 отображаются 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. Приложения "Лаборатории Касперского", использующиеся в вашей организации, получают обновленные данные о репутации объекта.

## Лучшие практики присвоения репутации приложениям

Обычно для запрещения или разрешения запуска приложений достаточно функций приложений "Лаборатории Касперского" – *Контроль приложений*. Контроль приложений позволяет настроить доступ к категориям приложений (например, играм) или отдельным приложениям по метаданным или другим данным. В результате запуск приложения будет заблокирован. Подробную информацию о работе Контроля приложений см. в документации к приложениям "Лаборатории Касперского".

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

Если вы используете собственные приложения, не подписанные доверенным сертификатом, вам нужно присвоить таким приложениям репутацию *Доверенный*. Присвоение приложению репутации *Доверенный* состоит из следующих этапов:

1. Добавьте сведения о собственном приложении в локальную репутационную базу.
2. В параметрах приложений "Лаборатории Касперского" добавьте категорию приложений: KL-категория / Другие приложения / Приложения, доверенные согласно репутации в KSN.
3. В параметрах Контроля приложений разрешите запуск приложений из новой категории.

## Особенности использования локальных репутационных баз

Kaspersky Private Security Network может использоваться с [разными приложениями "Лаборатории Касперского"](#). Определение репутации объектов из локальных репутационных баз может отличаться в зависимости от приложения "Лаборатории Касперского", установленного на компьютерах организации. Например, определение репутации объекта приложением может отличаться по следующим причинам:

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

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

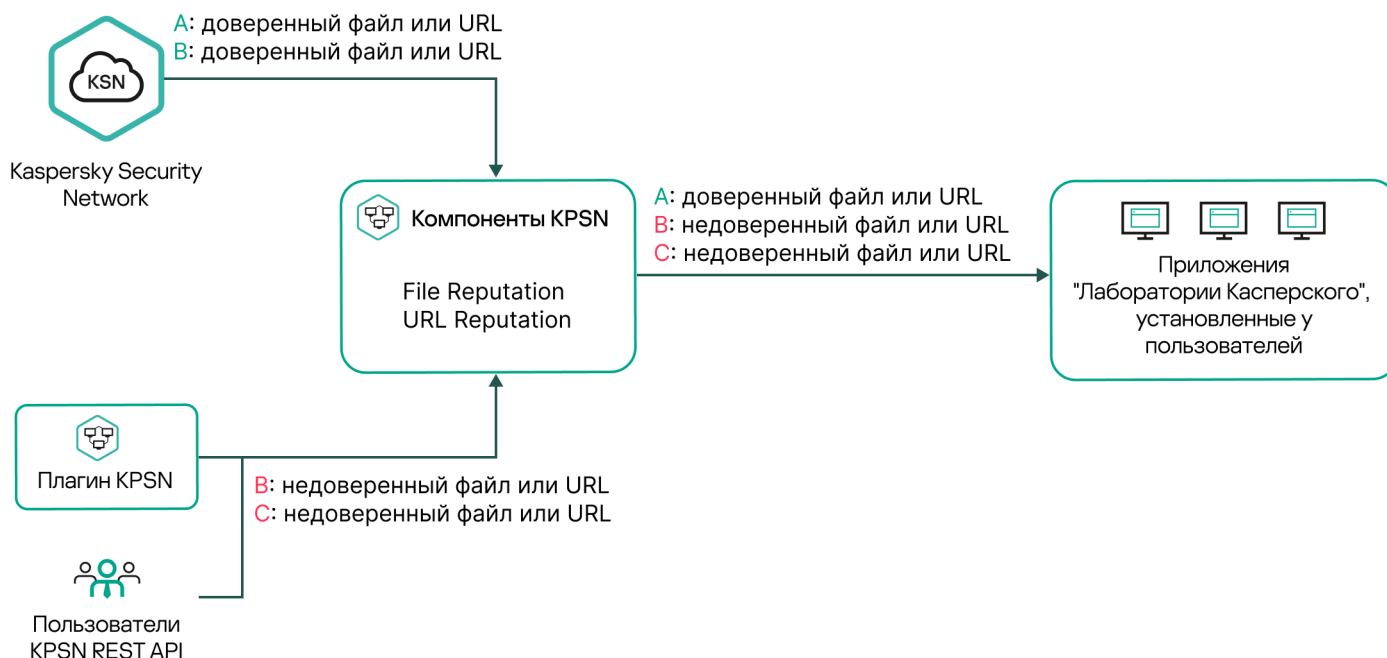


Схема работы администратора Kaspersky Private Security Network с локальными репутационными базами

## Добавление и обновление сведений о репутации файлов или веб-сайтов

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*.

В локальную репутационную базу Kaspersky Private Security Network можно добавлять сведения о репутации файлов и веб-сайтов по одному или одновременно о нескольких файлах или веб-сайтах.

Чтобы добавить или обновить сведения о репутации одного файла в локальной репутационной базе:

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Репутационные списки KPSN** → **File Reputation**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Репутационные списки** → **File Reputation**.

2. Нажмите на кнопку **Добавить** и выберите способ добавления файла:

- **Добавить хеш.**

В этом варианте вам понадобится хеш-сумма файла (MD5 или SHA256).

- **Импортировать файл.**

В этом варианте вам понадобится файл, для которого вы хотите добавить репутационную запись. Хеш-суммы этого файла будут определены автоматически.

3. В открывшемся окне укажите следующие данные:

а. В блоке параметров **Репутация** выберите репутацию, которую вы хотите присвоить файлу. Возможные значения:

- **Доверенный.**
- **Недоверенный.**

б. Если вы выбрали способ добавления **Добавить хеш**, в поле **Хеш** укажите хеш-сумму файла. Дополнительно можно заполнить поля **Имя файла** и **Описание**. Это необязательные поля.

в. Если вы выбрали способ добавления **Импортировать файл**, нажмите на кнопку **Обзор**, выберите файл сертификата и нажмите на кнопку **Отпр.**

Дополнительно можно заполнить поле **Описание** (необязательно).

4. Нажмите на кнопку **Сохранить**.

Откроется окно Контроля соответствия.

5. Сравните сведения о репутации файла из базы Kaspersky Security Network (столбец **KL-репутация**) и имеющиеся сведения в локальной репутационной базе (столбец **Текущая локальная репутация**) со вновь добавленными данными (столбец **Новая локальная репутация**). Примите решение о необходимости добавления новой информации о репутации файла (обновления репутации) в локальной репутационной базе.

6. Нажмите на кнопку **ОК**, если репутацию файла в локальной репутационной базе действительно нужно обновить.

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

*Чтобы добавить или обновить сведения о репутации нескольких файлов в локальной репутационной базе:*

1. Подготовьте список файлов:

а. Создайте текстовый файл (например, list\_for\_import.txt).

б. Добавьте список хешей файлов (MD5 или SHA256). В дополнение к хешу можно ввести имя файла (не более 256 символов) и его описание (не более 1024 символов). Хеш, имя и описание файла должны разделяться символом табуляции. Каждая запись должна начинаться с новой строки.

Пример:

|                                  |             |               |
|----------------------------------|-------------|---------------|
| 1BC29B36F623BA82AAF6724FD3B16718 | file name   | description   |
| AF6724FD3B167181BC29B36F623BA82A | file name 2 | description 2 |

Поддерживается добавление не более 1000 записей в один файл.

2. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Репутационные списки KPSN** → **File Reputation**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Репутационные списки** → **File Reputation**.

3. Нажмите на кнопку **Импорт списка**.

4. В открывшемся окне выполните следующие действия:

а. В блоке параметров **Репутация** выберите репутацию, которую вы хотите присвоить файлу. Возможные значения:

- **Доверенный.**
- **Недоверенный.**

Репутация будет присвоена всем файлам из списка.

б. Импортируйте подготовленный на первом шаге TXT-файл со списком файлов. Для этого выполните одно из действий:

- Перетащите TXT-файл в выделенную область.
- Нажмите на кнопку **Обзор**, выберите файл сертификата и нажмите на кнопку **Open**.

5. Нажмите на кнопку **Импорт**.

Откроется окно Контроля соответствия.

6. Сравните сведения о репутации файлов из базы Kaspersky Security Network (столбец **KL-репутация**) и имеющиеся сведения в локальной репутационной базе (столбец **Текущая локальная репутация**) со вновь добавленными данными (столбец **Новая локальная репутация**). Вы можете принять решение не добавлять новые сведения о репутации некоторых из файлов в локальной репутационной базе; в этом случае снимите флажок **Обновить** в строке того файла, репутацию которого обновлять не нужно.

7. Нажмите на кнопку **ОК**.

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

*Чтобы добавить или обновить сведения о веб-сайте в локальной репутационной базе:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Репутационные списки KPSN** → **URL Reputation**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Репутационные списки** → **URL Reputation**.

2. Нажмите на кнопку **Добавить**.

3. В открывшемся окне укажите следующие данные:

а. В блоке параметров **Репутация** выберите репутацию, которую вы хотите присвоить веб-сайту. Возможные значения:

- **Доверенный.**
- **Недоверенный.**
- URL веб-сайта. URL должен удовлетворять требованиям RFC 3986.

При добавлении URL в локальную репутационную базу обрезаются все части URL, кроме доменной части и пути. Символ "\*" используется как подстановочный символ: вместо одного или более символов.

- Описание (необязательно).

4. Нажмите на кнопку **Сохранить**.

Откроется окно Контроля соответствия.

5. Сравните сведения о репутации веб-сайта из базы Kaspersky Security Network (столбец **KL-репутация**) и имеющиеся сведения в локальной репутационной базе (столбец **Текущая локальная репутация**) со вновь добавленными данными (столбец **Новая локальная репутация**). Примите решение о необходимости добавления новой информации о репутации веб-сайта (обновления репутации) в локальной репутационной базе.

6. Нажмите на кнопку **ОК**, если репутацию веб-сайта в локальной репутационной базе действительно нужно обновить.

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

*Чтобы добавить или обновить сведения о нескольких веб-сайтах в локальной репутационной базе:*

1. Подготовьте список веб-сайтов:

a. Создайте текстовый файл (например, list\_for\_import.txt).

b. Добавьте список URL-адресов веб-сайтов. В дополнение к URL можно ввести описание веб-сайта (не более 1024 символов). URL и описание должны разделяться символом табуляции. Каждая запись должна начинаться с новой строки.

Пример:

|              |               |
|--------------|---------------|
| example.com  | description   |
| example2.com | description 2 |

Поддерживается добавление не более 1000 записей в один файл. URL должны удовлетворять требованиям RFC 3986, допускается использование маски (\*). При добавлении URL в локальную репутационную базу обрезаются все части URL, кроме доменной части и пути. Символ "\*" используется как подстановочный символ: вместо одного или более символов.

2. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Репутационные списки KPSN** → **URL Reputation**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Репутационные списки** → **URL Reputation**.

3. Нажмите на кнопку **Импорт списка**.

4. В открывшемся окне укажите следующие данные:

a. В блоке параметров **Репутация** выберите репутацию, которую вы хотите присвоить веб-сайтам. Возможные значения:

- **Доверенный.**
- **Недоверенный.**

Репутация будет присвоена всем веб-сайтам.

б. Импортируйте подготовленный на первом шаге TXT-файл со списком веб-сайтов. Для этого выполните одно из действий:

- Перетащите TXT-файл в выделенную область.
- Нажмите на кнопку **Обзор**, выберите файл сертификата и нажмите на кнопку **Open**.

5. Нажмите на кнопку **Импорт**.

Откроется окно Контроля соответствия.

6. Сравните сведения о репутации веб-сайтов из базы Kaspersky Security Network (столбец **KL-репутация**) и имеющиеся сведения в локальной репутационной базе (столбец **Текущая локальная репутация**) со вновь добавленными данными (столбец **Новая локальная репутация**). Вы можете принять решение не добавлять новые сведения о репутации некоторых из веб-сайтов в локальной репутационной базе; в этом случае снимите флажок **Обновить** в строке того веб-сайта, репутацию которого обновлять не нужно.

7. Нажмите на кнопку **ОК**.

Новые сведения о репутации добавленных веб-сайтов 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. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Репутационные списки KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Репутационные списки**.

- Если вы хотите экспортировать сведения о репутации файлов, выберите вкладку **File Reputation**.
- Если вы хотите экспортировать сведения о репутации веб-сайтов, выберите вкладку **URL Reputation**.

2. Нажмите на кнопку **Экспорт списка**:

- 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. В список будут включены все добавленные в локальную базу и не удаленные ранее объекты.

# Удаление записей о репутации файлов или веб-сайтов

Удаление записей о репутации файла или веб-сайта из локальной репутационной базы означает, что запись о файле или веб-сайте переводится в состояние "отключено" и становится недоступной для программ "Лаборатории Касперского", использующихся в вашей организации. Запись об этом файле или веб-сайте остается доступной в веб-интерфейсе плагина KPSN, ее можно включить после удаления.

*Чтобы удалить записи из локальной репутационной базы:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Репутационные списки KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Репутационные списки**.

Далее:

- Если вы хотите удалить сведения о репутации файлов, выберите вкладку **File Reputation**.
- Если вы хотите удалить сведения о репутации веб-сайтов, выберите вкладку **URL Reputation**.

2. Отключите выбранные записи одним из следующих способов:

- В строках тех записей, которые нужно отключить, в столбце **Статус** переведите переключатель в положение **Отключено**.
- Установите флажки в строках тех записей, которые нужно отключить, затем нажмите на кнопку **Статус** и выберите пункт **Отключить**.

Сведения о выбранных файлах или веб-сайтах будут удалены из локальной репутационной базы и станут недоступны для программ "Лаборатории Касперского", использующихся в вашей организации.

# Мониторинг работы Kaspersky Private Security Network

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

*Чтобы просмотреть общую информацию о работе Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Security Center Web Console в окне браузера.
2. Перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.

На странице панели мониторинга веб-виджет **Общий статус KPSN** отображает общий статус работоспособности Kaspersky Private Security Network, его компонентов и конфигурации.

Вы можете нажать на названия параметров в левой части веб-виджета **Общий статус KPSN**, чтобы перейти в разделы веб-плагина Kaspersky Private Security Network и узнать подробнее о его работе или возникших проблемах. Вы также можете перейти в раздел с графиками мониторинга Kaspersky Private Security Network, нажав на кнопку **Подробнее** в нижней части веб-виджета.

## Мониторинг состояния компонентов и серверов

Kaspersky Private Security Network автоматически проверяет состояние своих [компонентов](#) и серверов, контролируя следующие параметры:

- отставание баз по каждому из потоков данных на каждом сервере;
- состояние установленных компонентов Kaspersky Private Security Network;
- срок действия ключей шифрования трафика между Kaspersky Private Security Network и приложениями "Лаборатории Касперского";
- сроки действия удостоверяющего центра (англ. certificate authority, CA), используемого для выдачи сертификатов;
- срок действия сертификата сервера Kaspersky Private Security Network;
- срок действия сертификата для получения обновлений Kaspersky Private Security Network.

*Чтобы узнать статус компонентов Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Security Center Web Console в окне браузера.
2. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Мониторинг и отчеты** → **Графики KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Графики**.

### 3. Выберите вкладку **Общий статус**.

На странице отобразится таблица выполненных проверок работоспособности серверов и компонентов Kaspersky Private Security Network и их результатов. Результаты в таблице обновляются каждые 30 секунд.

### 4. При необходимости отфильтруйте строки в таблице выполненных проверок:

- Чтобы просмотреть результаты проверок определенных серверов, нажмите на заголовок столбца **Сервер** и выберите в раскрывающемся списке необходимые сервера.
- Чтобы найти строки, которые содержат определенный текст, в поле **Поиск** справа над таблицей введите текст для поиска и нажмите **Enter**.

В таблице отобразятся только те строки, которые содержат введенный текст хотя бы в одном столбце. Поиск текста осуществляется по значениям во всех ячейках.

В таблице проверок отображается следующая информация:

- **Сервер** – IP-адрес и порт или название сервера, если проверка относится к конкретному серверу. Если проверка относится к Kaspersky Private Security Network в целом, сервер не указывается.
- **Объект** – название проверки Kaspersky Private Security Network: например по названию низкоуровневого компонента или потока обновлений.
- **Статус** – результат проверки Kaspersky Private Security Network. Может быть **ОК**, если проверка не выявила ошибок, либо текст обнаруженной ошибки.

## Мониторинг репутации объектов

Вы можете просмотреть статистику ответов о репутации объектов, которые [компоненты File Reputation и URL Reputation](#) предоставили на запросы приложений "Лаборатории Касперского".

*Чтобы просмотреть статистику ответов от компонентов Kaspersky Private Security Network на запросы приложений "Лаборатории Касперского":*

1. Откройте веб-интерфейс Kaspersky Security Center Web Console в окне браузера.
2. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Мониторинг и отчеты** → **Графики KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Графики**.
3. Выберите вкладку **Ответы**.
4. В раскрывающемся списке временных интервалов выберите интервал, за который вы хотите просмотреть информацию о работе компонентов.

На комплексной странице отобразятся графики для [компонентов Kaspersky Private Security Network](#). Графики статистики ответов от компонентов File Reputation и URL Reputation за выбранный период времени располагаются в соответствующих блоках. Если у вас установлен только один из этих компонентов, на странице отобразится только блок графиков для этого компонента.

Страница статистики ответов доступна, только если у вас установлен хотя бы один из компонентов File Reputation или URL Reputation.

В каждом блоке отображается следующая информация:

- общее количество запросов к компоненту;
- количество ответов об объектах с хорошей, плохой и неизвестной репутацией, полученной от компонента и из локальной репутационной базы;
- круговая диаграмма и гистограмма, иллюстрирующие статистику ответов.

В Kaspersky Private Security Network версии 4.0.1 и выше вы можете включить автообновление содержимого отображаемых графиков. Для этого включите переключатель **Обновлять автоматически**. График будет автоматически обновляться раз в 30 секунд согласно выбранному вами интервалу. Также вы можете обновить содержимое отображаемых графиков вручную.

### Круговая диаграмма репутации объектов

С помощью круговой диаграммы вы можете контролировать процентное отношение ответов об объектах с хорошей, плохой и неизвестной репутацией от компонентов File Reputation или URL Reputation и локальной репутационной базы к общему числу ответов.

Вы можете установить или снять флажки в левой части блока напротив ответов, чтобы отображать статистику только по ответам с выбранной репутацией на графиках.

Вы можете скрыть круговую диаграмму, сняв флажок **Круговая диаграмма**.

### Гистограмма ответов о репутации объектов

С помощью гистограммы вы можете контролировать количество ответов об объектах с хорошей, плохой и неизвестной репутацией от компонентов File Reputation или URL Reputation, а также локальной репутационной базы, по времени.

Высота и цвет каждого столбца гистограммы отображает количество ответов в конкретный временной промежуток. Вы можете установить или снять флажки в левой части блока напротив ответов, чтобы отображать статистику только по ответам с выбранной репутацией на графиках.

## Мониторинг времени обработки запросов

Для контроля работоспособности компонентов вы можете просматривать время, за которое компоненты Kaspersky Private Security Network обрабатывают запросы от приложений "Лаборатории Касперского".

Чтобы просмотреть время обработки запросов компонентами Kaspersky Private Security Network:

1. Откройте веб-интерфейс Kaspersky Security Center Web Console в окне браузера.
2. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Мониторинг и отчеты** → **Графики KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Графики**.
3. Выберите вкладку **Скорость обработки запросов**.
4. В раскрывающемся списке временных интервалов выберите интервал, за который вы хотите просмотреть информацию о работе компонентов.

На комплексной странице отобразятся графики для [компонентов Kaspersky Private Security Network](#).  
Графики для каждого из компонентов Kaspersky Private Security Network, которые установлены на сервере, отображаются в соответствующих блоках. Состав отображаемых графиков и диаграмм зависит от конфигурации Kaspersky Private Security Network и подключенных потоков данных.

В каждом блоке отображается следующая информация:

- общее количество обработанных запросов;
- количество запросов, обработанных компонентом за определенное время или не обработанных из-за ошибки;
- круговая диаграмма и гистограмма, иллюстрирующие статистику времени обработки запросов.

В Kaspersky Private Security Network версии 4.0.1 и выше вы можете включить автообновление содержимого отображаемых графиков. Для этого включите переключатель **Обновлять автоматически**. График будет автоматически обновляться раз в 30 секунд согласно выбранному вами интервалу. Также вы можете обновить содержимое отображаемых графиков вручную.

### Круговая диаграмма времени обработки запросов

С помощью круговой диаграммы вы можете контролировать процентное отношение количества запросов к компоненту, обработанных за определенное время или не обработанных из-за ошибки, к общему числу запросов к компоненту.

Вы можете установить или снять флажки в левой части блока напротив временных промежутков, чтобы отображать статистику только по запросам, обработанным за это время.

### Гистограмма скорости обработки запросов по времени

С помощью гистограммы вы можете контролировать количество запросов к компоненту, обработанных за определенное время или не обработанных из-за определенной ошибки за выбранный период.

Высота каждого столбца соответствует общему числу запросов, обработанных за указанное время или не обработанных из-за ошибки, а цвет – количеству запросов, которые были обработаны за указанное время или не обработаны. Вы можете установить или снять флажки в левой части блока напротив временных интервалов, чтобы отображать статистику только по запросам, обработанным за это время.

## Скорость обработки запросов

По графикам вы можете оценить работоспособность компонентов Kaspersky Private Security Network по скорости, с которой они обрабатывают запросы. Области графика заполняются цветом согласно цвету, указанному в блоке описания временных промежутков.

# Мониторинг отставания обновляемых баз

*Чтобы контролировать время отставания обновляемых баз компонентов Kaspersky Private Security Network:*

1. Откройте веб-интерфейс Kaspersky Security Center Web Console в окне браузера.
2. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Мониторинг и отчеты** → **Графики KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Графики**.
3. Выберите вкладку **Обновление баз KPSN**.
4. В раскрывающемся списке временных интервалов выберите интервал, за который вы хотите просмотреть информацию о работе компонентов.

На комплексной странице отобразятся графики отставания баз для сервисов Kaspersky Private Security Network.

Графики каждого из компонентов Kaspersky Private Security Network, установленных на сервере, отобразятся в соответствующих блоках. Состав отображаемых графиков и диаграмм зависит от конфигурации Kaspersky Private Security Network.

По графику вы можете просматривать время отставания баз Kaspersky Private Security Network от баз Kaspersky Security Network, чтобы контролировать качество связи. Высота каждой точки на графике соответствует времени отставания локальной репутационной базы компонента от Kaspersky Security Network.

Если вы установили несколько одинаковых компонентов Kaspersky Private Security Network, эти компоненты отображаются отдельными линиями на одном графике. Подпись к линии соответствует имени сервера. По этим линиям вы можете сравнивать отставание в получении пакетов между одинаковыми компонентами. При необходимости вы можете снять флажки в нижней части блока с графиком компонента, чтобы скрыть линии компонентов на других серверах.

В Kaspersky Private Security Network версии 4.0.1 и выше вы можете включить автообновление содержимого отображаемых графиков. Для этого включите переключатель **Обновлять автоматически**. График будет автоматически обновляться раз в 30 секунд согласно выбранному вами интервалу. Также вы можете обновить содержимое отображаемых графиков вручную.

# 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 ключами шифрования трафика

*Чтобы устранить неполадки с ключами шифрования трафика:*

1. Загрузите или создайте новый [ключ шифрования трафика](#).
2. [Получите новый конфигурационный файл Kaspersky Private Security Network](#) и передайте его в приложения, которые используют Kaspersky Private Security Network.

## Неполадки, связанные с сертификатами для получения обновлений

*Чтобы устранить неполадки, связанные с сертификатами обновления,*

[запросите новый сертификат](#) у специалистов "Лаборатории Касперского" (в соответствии с лицензией вашей организации).

## Неполадки, связанные с активностью компонентов

*Чтобы устранить неполадки, связанные с активностью компонентов,*

убедитесь, что сервер соответствует [аппаратным требованиям](#).

## Неполадки, связанные с отставанием обновления баз

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

1. Убедитесь, что сервер соответствует [аппаратным требованиям](#).
2. Убедитесь, что не истек срок действия сертификата 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](#).
2. Убедитесь, что количество продуктов, подключенных к Kaspersky Private Security Network, [соответствует конфигурации](#).
3. Убедитесь, что к Kaspersky Private Security Network подключены продукты поддерживаемых версий.

# Оповещения о событиях в работе Kaspersky Private Security Network

Вы можете настроить следующие виды оповещений:

- почтовые оповещения о событиях в работе Kaspersky Private Security Network;
- добавление в Syslog записи о событии в работе Kaspersky Private Security Network.

При необходимости получать почтовые оповещения вам следует самостоятельно подготовить SMTP-сервер.

При необходимости вести записи в syslog вам следует самостоятельно подготовить syslog-сервер.

Оповещения могут формироваться для следующих видов событий:

- Окончание срока годности ключей шифрования трафика.

Оповещение формируется, если срок действия ключа шифрования трафика истек или составляет менее двух недель.

- Окончание срока годности используемых сертификатов.

Оповещение формируется в следующих случаях:

- Срок действия сертификата для получения обновлений истек или составляет менее двух недель.
- Срок действия сертификата сервера Kaspersky Private Security Network истек или составляет менее месяца.
- Срок действия удостоверяющего центра, используемого для выдачи сертификатов, истек или составляет менее месяца.

- Ошибки компонентов KPSN.

Оповещение формируется, если компонент внезапно завершил работу и не запустился в течение двух минут или произошло более одного внезапного завершения работы за две минуты.

- Отставание баз данных.

Оповещение формируется, если превышен порог отставания базы данных сервиса.

- Ошибки обработки запросов.

Оповещение формируется, если произошли ошибки при обработке запросов от приложений, использующих Kaspersky Private Security Network.

# Настройка почтовых оповещений о событиях в работе Kaspersky Private Security Network

При необходимости получать почтовые оповещения вам следует самостоятельно подготовить SMTP-сервер.

*Чтобы настроить получение оповещений о событиях в работе Kaspersky Private Security Network по электронной почте:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.  
В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.
2. На вкладке **Оповещения** в блоке **Оповещения** в таблице событий в колонке **Email** установите флажки в строках тех событий, о которых вы хотите получать оповещения.
3. В блоке **Параметры почтового сервера** нажмите на кнопку **Параметры** для настройки параметров соединения с почтовым сервером.
4. В открывшемся окне **Параметры почтового сервера** установите параметры почтового оповещения:
  - a. В поле **Адрес SMTP-сервера** укажите адрес почтового сервера вашей организации (например, smtp.example.com).
  - b. В поле **Порт SMTP-сервера** укажите порт почтового сервера вашей организации (например, 25).
  - c. В раскрывающемся списке **Аутентификация клиента** выберите тип аутентификации.  
Возможные значения: **Без аутентификации**, **По логину и паролю**, **По сертификату**.
  - d. Если вы выбрали аутентификацию по логину и паролю, в полях **Логин** и **Пароль** ведите учетные данные для аутентификации.
  - e. Если вы выбрали аутентификацию по сертификату:
    1. В раскрывающемся списке **Формат сертификата клиента** выберите формат файла сертификата, который будет использоваться для аутентификации.
    2. В поле **Пароль сертификата клиента** введите пароль сертификата. Это необязательное поле.
    3. Нажмите на кнопку **Обзор** и выберите файл сертификата с расширением CRT, CER, PEM или DER.
    4. Если вы выбрали формат сертификата **X.509**, нажмите на кнопку **Обзор** и выберите файл закрытого ключа формата KEY или PEM.
  - f. В раскрывающемся списке **Версия TLS** выберите, какую версию TLS следует использовать при подключении к почтовому серверу.  
Возможные значения: **Не использовать TLS**, **Использовать TLS 1.2 и выше**.

Если вы не хотите использовать TLS-протокол, выберите значение **Не использовать TLS**. Это значение доступно, только если для поля **Аутентификация клиента** выбрано значение **Без аутентификации**.

g. Если вы выбрали использование TLS-протокола, нажмите на кнопку **Обзор** и выберите файл доверенного сертификата 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.

h. В поле **Адрес отправителя** введите адрес электронной почты или имя, которые будут указаны в качестве отправителя почтового оповещения.

i. В поле **Язык** выберите язык, который будет использован в оповещениях.

j. Нажмите на кнопку **Сохранить**.

5. Для проверки соединения с почтовым сервером нажмите на кнопку **Отправить тестовое письмо**, в открывшемся окне укажите адрес электронной почты, на который можно отправить проверочное письмо, и нажмите на кнопку **Отправить тестовое письмо**.

Если письмо не приходит, проверьте параметры почтового сервера и попробуйте отправить письмо снова.

6. Укажите получателей почтовых оповещений о событиях в работе Kaspersky Private Security Network:

a. Нажмите на кнопку **Указать получателей**.

b. В поле **Получатели оповещений** введите адрес электронной почты получателя оповещений. Можно указать несколько адресов, разделяя их запятой (,) или точкой с запятой (;).

c. Нажмите на кнопку **Сохранить**.

Почтовые оповещения о событиях в работе Kaspersky Private Security Network будут настроены.

## Настройка записи в Syslog событий в работе Kaspersky Private Security Network

При необходимости вести записи в Syslog вам следует самостоятельно подготовить Syslog-сервер.

*Чтобы настроить запись в Syslog сведений об событиях в работе Kaspersky Private Security Network:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

2. На вкладке **Оповещения** в блоке **Оповещения** в таблице событий в колонке **Syslog** установите флажки в строках тех событий, о которых вы хотите получать оповещения.

3. В блоке **Параметры Syslog** нажмите на кнопку **Параметры**.

4. В открывшемся окне установите параметры соединения с Syslog-сервером:

- a. В поле **Адрес** укажите URL или IPv4-адрес Syslog-сервера.
- b. В поле **Порт** укажите порт для подключения к Syslog-серверу.
- c. В поле **Протокол** укажите используемый для соединения протокол. Возможные значения: **UDP, TCP**.
- d. Нажмите на кнопку **Сохранить**.

Сведения о событиях в работе Kaspersky Private Security Network будут добавляться в журнал Syslog с тегом *KPSN*.

Формат оповещений об ошибках в работе компонентов Kaspersky Private Security Network, добавляемых в Syslog: <Дата и время> <Адрес сервера> kpsn <Сообщение об ошибке>.

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

# API KPSN

*Программный интерфейс Kaspersky Private Security Network* (далее также "API KPSN" или просто "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](#).

Запросы к API выполняются только по протоколу HTTPS. Для аутентификации пользователей используются клиентские сертификаты.

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.

В одном запросе должно быть не более 1000 элементов.

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

## Подготовка к использованию API

*Чтобы начать использовать API KPSN:*

1. Убедитесь, что у вашей учетной записи есть доступ на использование API.

Если вы планируете изменять сведения о репутации файлов или веб-сайтов, вам также необходим доступ к управлению локальной репутационной базой файлов и веб-сайтов.

[Управление правами доступа выполняется в Kaspersky Security Center Web Console](#).

2. Получите сертификаты и ключ для аутентификации клиента:

- a. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN** → **Доступ к API**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры** → **Доступ к API**.

- b. Нажмите на кнопку **Получить сертификат для API**.

Kaspersky Private Security Network загрузит ZIP-архив в директорию для загрузки по умолчанию.

Загруженный архив содержит следующие файлы:

- *client\_certificate.pem* – ваш клиентский сертификат для использования API.
- *private\_key.pem* – ваш закрытый ключ для использования API.
- *ca\_certificate.pem* – публичный сертификат CA. Вы можете его использовать для проверки сертификата сервера Kaspersky Private Security Network.

### 3. Узнайте адреса, по которым доступен API KPSN.

Эти адреса указаны в разделе **Доступ к API**, блок **Параметры доступа к API**. Вы можете использовать любой из указанных адресов.

## Выполнение запросов к API

*Чтобы выполнять запросы к API:*

1. Ранее [скачанный ZIP-архив с сертификатом и ключом](#) распакуйте на компьютер, с которого будут выполняться запросы к API.
2. Добавьте ваш клиентский сертификат (*client\_certificate.pem*) и закрытый ключ (*private\_key.pem*) в параметрах аутентификации REST-клиента, если не хотите их указывать непосредственно в запросах.
3. При необходимости добавьте публичный сертификат CA (*ca\_certificate.pem*) в список CA, используемый REST-клиентом.

В каждом запросе к API необходимо указывать заголовок "Content-Type: application/json".

### Пример запроса с указанием ключа и сертификата

```
curl --cert <certificate> --key <key> -X POST -H "Content-Type: application/json" -d
<data> <KPSN API Address>
```

Здесь:

<certificate> – путь к вашему клиентскому сертификату.

<key> – путь к вашему закрытому ключу.

<data> – тело запроса в формате JSON, примеры приведены в следующих разделах.

<KPSN API Address> – адрес KPSN, по которому доступен API.

# 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, в ответе будет 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 по используемому адресу Kaspersky Private Security Network.
  2. В списке методов выберите метод POST.
  3. В поле адреса запроса введите адрес, по которому доступен API KPSN.
  4. В рабочей области введите тело запроса в формате JSON. См. пример ниже.
  5. Отправьте запрос сервису File Reputation.
- В окне REST-клиента отобразится ответ с результатом выполнения запроса.

Пример тела 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 (\*). При добавлении URL в локальную репутационную базу обрезаются все части URL, кроме доменной части и пути. Символ "\*" используется как подстановочный символ: вместо одного или более символов.
  - `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 по используемому адресу Kaspersky Private Security Network.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите адрес, по которому доступен API KPSN.
4. В рабочей области введите тело запроса в формате JSON. См. пример ниже.
5. Отправьте запрос сервису URL Reputation.  
В окне REST-клиента отобразится ответ с результатом выполнения запроса.

Пример тела 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, в ответе будет 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 по используемому адресу Kaspersky Private Security Network.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите адрес, по которому доступен API KPSN.
4. В рабочей области введите тело запроса в формате JSON. См. пример ниже.

5. Отправьте запрос сервису File Reputation.

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

Пример тела 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 требованиям RFC 3986. При добавлении URL в локальную репутационную базу обрезаются все части URL, кроме доменной части и пути. Символ "\*" используется как подстановочный символ: вместо одного или более символов.

*Чтобы удалить сведения о репутации веб-сайта:*

1. Запустите REST-клиент на любом компьютере локальной сети организации, имеющем доступ к серверу по используемому адресу Kaspersky Private Security Network.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите адрес, по которому доступен API KPSN.
4. В рабочей области введите тело запроса в формате JSON. См. пример ниже.
5. Отправьте запрос сервису URL Reputation.
6. В окне REST-клиента отобразится ответ с результатом выполнения запроса.

Пример тела 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, в ответе будет 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 по используемому адресу Kaspersky Private Security Network.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите адрес, по которому доступен API KPSN.
4. В рабочей области введите тело запроса в формате JSON. См. пример ниже.
5. Отправьте запрос сервису File Reputation.

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

## Пример тела 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: <ul style="list-style-type: none"><li>• 0 – неизвестный;</li><li>• 1 – доверенный;</li><li>• 2 – недоверенный;</li><li>• -1 – неопределенный.</li></ul>                                                                                                                                                       | Да                   |
| description  | Дополнительные сведения о репутации файла.                                                                                                                                                                                                                                                                                                         | Нет                  |
| product      | Название приложения, которому 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 приложений "Лаборатории Касперского", отправляющих данные в Kaspersky Security Network.<br>Группы доверия: <ul style="list-style-type: none"><li>• trusted – доверенный;</li><li>• untrusted – недоверенный;</li><li>• low – сильные ограничения;</li><li>• high – слабые ограничения.</li></ul> | Нет                  |
| geoSharing   | Процентное распределение обнаружений файла по странам.<br>Страны указываются в виде двухбуквенного кода. 00 означает сведенную в одну категорию статистику по нескольким странам.                                                                                                                                                                  | Нет                  |
| client_data  | Идентификатор источника информации в ответе: <ul style="list-style-type: none"><li>• true – репутация из источников вашей организации;</li><li>• false – репутация из баз Kaspersky Private Security Network.</li></ul>                                                                                                                            | 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
 }
 }
]
}

```

## 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 требованиям RFC 3986.

*Чтобы проверить репутацию веб-сайта:*

1. Запустите REST-клиент на любом компьютере локальной сети организации, имеющем доступ к серверу по используемому адресу Kaspersky Private Security Network.
2. В списке методов выберите метод POST.
3. В поле адреса запроса введите адрес, по которому доступен API KPSN.
4. В рабочей области введите тело запроса в формате JSON. См. пример ниже.
5. Отправьте запрос сервису URL Reputation.

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

### Пример тела 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: <ul style="list-style-type: none"><li>• 0 – неизвестный;</li><li>• 1 – доверенный;</li><li>• 2 – недоверенный;</li><li>• -1 – неопределенный.</li></ul>                        | Да                   |
| ttl         | Рекомендуемое время (в секундах), на которое клиент может закешировать полученный ответ                                                                                                                                 | Да                   |
| categories  | Список с идентификаторами категорий <a href="#">веб-сайта</a> . Если информация по запрошенному веб-адресу отсутствует, выводится пустой список.                                                                        | Да                   |
| client_data | Идентификатор источника информации в ответе: <ul style="list-style-type: none"><li>• true – репутация из источников вашей организации;</li><li>• false – репутация из баз Kaspersky Private Security Network.</li></ul> | Да                   |

Пример ответа:

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

## Коды ошибок

Во время работы с API возможны сбои в работе Kaspersky Private Security Network. Каждой ошибке присвоен код (см. таблицу ниже). Все ошибки содержатся в теле ответа, кроме ошибки с кодом 401.

| 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 <code>action</code> может быть указано значение <code>check_url</code> , а не <code>chec1_url</code> .                                                |
| 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.                                                                                                                                |
| 6          | Слишком много записей в запросе (общее).                                        | Убедитесь, что в запросе содержится не более 1000 записей. При необходимости разделите запрос на несколько.                                                                                                         |
| 51         | У пользователя недостаточно прав (авторизация).                                 | Проверьте наличие необходимых <a href="#">прав пользователя</a> .                                                                                                                                                   |
| 53         | Неправильные учетные данные (аутентификация).                                   | Повторно <a href="#">получите сертификат и ключ для API</a> .                                                                                                                                                       |
| 101        | Недопустимая репутация объекта (локальная репутационная база).                  | Убедитесь, что значение параметра репутации объекта ( <code>reputation</code> ) указано верно. Возможные значения: <ul style="list-style-type: none"> <li>• 1 – доверенный;</li> <li>• 2 – недоверенный.</li> </ul> |
| 151        | Короткий URL-адрес (URL Reputation).                                            | Убедитесь, что URL-адрес соответствует RFC 3986. Введите URL-адрес по шаблону <code>example.com</code>                                                                                                              |
| 152        | Недопустимый URL-адрес веб-сайта (URL Reputation).                              | Убедитесь, что URL-адрес соответствует RFC 3986. Введите URL-адрес по шаблону <code>example.com</code>                                                                                                              |
| 153        | URL-адрес не удалось обработать (URL Reputation).                               | Убедитесь, что URL-адрес соответствует RFC 3986. Введите URL-адрес по шаблону <code>example.com</code>                                                                                                              |
| 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 ( <code>hash</code> ). 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 ( <code>hash_type</code> ) указан верно.                                                                                                                              |
| 204        | Неизвестный алгоритм хеширования (File Reputation).                             | Убедитесь, что для параметра алгоритма хеширования ( <code>hash_type</code> ) указано значение MD5 и SHA256. Kaspersky Private Security Network не поддерживает другие алгоритмы хеширования.                       |
| 255        | Неизвестная ошибка (общее).                                                     | Обратитесь в Службу технической поддержки.                                                                                                                                                                          |
| 401        | Клиентский сертификат не предоставлен или является невалидным (аутентификация). | Повторно <a href="#">получите сертификат и ключ для API</a> .                                                                                                                                                       |

# Журнал Kaspersky Private Security Network

Журнал Kaspersky Private Security Network предназначен для диагностики и решения возникших проблем в работе приложения. 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 на сервере, на котором установлена серверная часть 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 приложений "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 приложений "Лаборатории Касперского":
  - Идентификатор компьютера, на котором установлено приложение "Лаборатории Касперского".
  - Идентификатор пользователя приложения "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.](#)

В журнале Kaspersky Private Security Network хранятся данные за последние 15 дней.

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

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

*Чтобы включить или выключить запись в журнал запросов для сервиса URL Reputation или File Reputation:*

1. В веб-интерфейсе Kaspersky Security Center Web Console 14.2 перейдите в раздел **Операции** → **Параметры KPSN**.

В веб-интерфейсе Kaspersky Security Center Web Console другой версии перейдите в раздел **Программы и службы** → **KPSN** → **Параметры**.

2. На вкладке **Конфигурация** в блоке **Конфигурация KPSN** выберите компонент **File Reputation** или **URL Reputation**.

3. В открывшемся окне с информацией о компоненте выполните одно из действий:

- Если вы хотите включить запись запросов, включите переключатель **Включить журналирование запросов**.
- Если вы хотите отключить запись запросов, выключите переключатель **Включить журналирование запросов**.

4. Нажмите на кнопку **Сохранить**.

Запись запросов для сервиса URL Reputation или File Reputation будет включена или отключена.

# Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

## Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Private Security Network, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Private Security Network.

Kaspersky предоставляет поддержку Kaspersky Private Security Network в течение жизненного цикла (см. [страницу жизненного цикла приложений](#)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с [правилами предоставления технической поддержки](#).

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

- [посетить сайт Службы технической поддержки](#);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с [портала Kaspersky CompanyAccount](#).

## Техническая поддержка через Kaspersky CompanyAccount

[Kaspersky CompanyAccount](#) – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;

- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на [веб-сайте Службы технической поддержки](#)<sup>2</sup>.

# Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

## Список портов для работы Kaspersky Private Security Network

Ниже перечислены порты, которые требуется открыть для работы Kaspersky Private Security Network на серверах, предназначенных для установки серверной части Kaspersky Private Security Network.

Порты, необходимые для работы Kaspersky Private Security Network

| Инициатор соединения                                | Цель соединения                                                                                  | Порт  | Протокол | Описание                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------|-------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Веб-плагин Kaspersky Security Center Web Console    | Сервер Kaspersky Private Security Network                                                        | 443   | HTTPS    | Управление Kaspersky Private Security Network                                                                                                                                                                                                                                                                                                                                                        |
| Клиент REST API                                     | Сервер Kaspersky Private Security Network                                                        | 80    | HTTPS    | Использование KPSN REST API                                                                                                                                                                                                                                                                                                                                                                          |
| Клиент REST API                                     | Сервер Kaspersky Private Security Network                                                        | 443   | HTTPS    | Использование KPSN REST API                                                                                                                                                                                                                                                                                                                                                                          |
| Приложение "Лаборатории Касперского"                | Сервер Kaspersky Private Security Network                                                        | 1443  | KSN      | Запросы приложений к сервисам Kaspersky Private Security Network                                                                                                                                                                                                                                                                                                                                     |
| Серверы Kaspersky Private Security Network          | Управляющий узел Kubernetes, на котором выполнялась установка Kaspersky Private Security Network | 31000 | TCP      | Доступ к локальному репозиторию контейнеров для развертывания компонентов Kaspersky Private Security Network.<br><br>Доступ по внешнему адресу Управляющего узла Kubernetes не требуется. Для каждого сервера достаточно доступа по указанному порту к этому же серверу (по localhost).<br><br>Также для взаимодействия с локальным репозиторием используется внутренняя сеть Kubernetes (см. ниже). |
| Серверы KPSN (адреса во внутренней сети Kubernetes) | Серверы KPSN (адреса во внутренней сети Kubernetes)                                              | Любой | Любой    | Взаимодействие компонентов Kaspersky Private Security Network внутри Kubernetes-кластера.<br><br>Используемые сети зависят от конфигурации Kubernetes. По умолчанию: 10.42.0.0/16, 10.43.0.0/16.<br><br>Подробнее см. документацию к K3s.                                                                                                                                                            |
| Серверы Kaspersky Private Security Network          | Управляющий узел Kubernetes, на котором выполнялась установка Kaspersky Private Security Network | 6443  | TCP      | Взаимодействие компонентов Kaspersky Private Security Network с k3s                                                                                                                                                                                                                                                                                                                                  |
| Серверы Kaspersky Private Security Network          | Серверы Kaspersky Private Security Network                                                       | 8472  | UDP      | Взаимодействие компонентов Kaspersky Private Security Network с k3s.<br><br>Порт указан для случая использования в Kubernetes сети Flannel VXLAN. Подробнее см. документацию к k3s.                                                                                                                                                                                                                  |

Для получения обновлений баз и запроса конфигурационных файлов разрешите исходящее соединение на ksn-pub-5.kaspersky-labs.com на порт 443 для следующих серверов:

- Для всех серверов с компонентами приложения, если вы используете стандартную конфигурацию Kaspersky Private Security Network.
- Для сервера с компонентом Gateway External, если вы используете Kaspersky Private Security Network с однонаправленным шлюзом.

# Список категорий веб-сайтов сервиса URL Reputation

Проверка репутации веб-сайтов с помощью HTTP-запроса к 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.

Категории веб-сайтов сервиса URL Reputation

| Идентификатор | Категория веб-сайта                     | Описание категории                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0             | Категория не присвоена                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 1             | Для взрослых                            | <p>Категория включает следующие типы материалов:</p> <ul style="list-style-type: none"><li>Веб-страницы, содержащие любые фото-, видео- или текстовые материалы с изображением или описанием половых органов людей или человекоподобных существ, полового акта или самоудовлетворения, совершенного людьми или человекоподобными существами.</li><li>Веб-страницы, содержащие эротические материалы, произведения, натуралистично описывающие половую жизнь человека, или произведения искусства, призванные вызывать сексуальное возбуждение.</li><li>Веб-страницы, посвященные обсуждению сексуальности в человеческих отношениях. Веб-страницы, посвященные каким-либо сексуальным практикам.</li><li>Веб-страницы, посвященные нудизму, в том числе сайты сообществ, сайты о местах отдыха для нудистов, размещающие нудистские фотографии.</li><li>Веб-страницы, посвященные сексуальному образованию.</li><li>Веб-страницы, предлагающие сексуальные услуги (онлайн или офлайн) и знакомства для секса, включая виртуальный секс.</li><li>Веб-страницы, рекламирующие или продающие предметы для секса и стимулирования сексуального возбуждения.</li><li>Веб-страницы, содержащие информацию об абортах.</li></ul> <p>См. также <b>Исключения</b> под таблицей.</p> |
| 3             | Алкоголь, табак, наркотики и психотропы | <p>Категория включает веб-ресурсы, содержание которых прямым или косвенным образом связано с алкогольной и спиртосодержащей продукцией, табачными изделиями, электронными сигаретами и наркотическими, психотропными или одурманивающими веществами.</p> <p>См. также <b>Исключения</b> под таблицей.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 4             | Насилие                                 | <p>Категория включает следующие типы материалов:</p> <ul style="list-style-type: none"><li>Веб-страницы, содержащие любые фото-, видео и текстовые материалы, которые описывают или изображают физическое или психологическое насилие над людьми или жестокое обращение с животными.</li><li>Веб-страницы, содержащие описания или изображения убийств, драк, пыток, изнасилований и издевательств над людьми, животными или вымышленными существами.</li><li>Веб-страницы, содержащие описания или изображения жертв и ужасов войны, вооруженных конфликтов, а также другие изображения страдающих людей.</li><li>Веб-страницы, содержащие тревожащие или огорчающие материалы, такие как изображение кровавых сцен, увечий, страшных аварий и прочее.</li><li>Веб-страницы, поощряющие причинение себе вреда или самоубийство либо действия, которые представляют угрозу жизни или здоровью.</li><li>Веб-страницы, содержащие информацию о расстройствах пищевого поведения, поощряющие их или содержащие обсуждение их в одобрительном ключе.</li><li>Веб-страницы, связанные с международно признанными террористическими, экстремистскими или расистскими организациями.</li></ul> <p>См. также <b>Исключения</b> под таблицей.</p>                                   |
| 5             | Нецензурная лексика                     | <p>Категория включает веб-ресурсы, содержащие нецензурную лексику.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|    |                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6  | Оружие, взрывчатые вещества, пиротехника | <p>Категория включает веб-ресурсы, содержащие информацию о вооруженных силах, оружии, взрывчатых веществах и пиротехнической продукции. Под "оружием" понимаются устройства и предметы, предназначенные для нанесения вреда жизни и здоровью людей и животных или для вывода из строя техники и сооружений. Сюда же относятся реплики оружия.</p> <p>Категория включает следующие типы материалов:</p> <ul style="list-style-type: none"> <li>Веб-сайты производителей и магазинов оружия, взрывчатых веществ, пиротехнической продукции и сопутствующих аксессуаров.</li> <li>Веб-страницы, посвященные изготовлению и использованию оружия, взрывчатых веществ, пиротехнической продукции и сопутствующих аксессуаров.</li> <li>Веб-страницы, содержащие товары для охоты и выживания (например, ножи, наборы для выживания, колющее оружие, кинжалы и прочее).</li> <li>Веб-страницы о стрелковом спорте и оружии для страйкбола.</li> <li>Веб-страницы, содержащие аналитические, исторические и производственные материалы, посвященные оружию, взрывчатым веществам и пиротехнической продукции.</li> <li>Веб-страницы, содержащие информацию на военную тематику, о тактическом снаряжении, описания вооруженных сил, групп и конфликтов, военных подрядчиков и военных доктрин.</li> </ul> <p>См. также <b>Исключения</b> под таблицей.</p> |
| 8  | Чаты, форумы, IM                         | Категория включает веб-ресурсы, предназначенные для публичного обсуждения различных тем с помощью специальных веб-приложений, а также веб-ресурсы, предназначенные для распространения и поддержки приложений для мгновенного обмена сообщениями, предоставляющих возможность коммуникации в реальном времени.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 9  | Веб-почта                                | <p>Категория включает страницы авторизации в почтовых сервисах и страницы почтового ящика, содержащего почтовые сообщения и сопутствующие данные (например, личные контакты). Категория не включает другие веб-страницы интернет-провайдера, предлагающего почтовый сервис.</p> <p>Содержание электронных писем исключается из других категорий (то есть содержание электронных писем не категоризируется).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 10 | Интернет-магазины                        | Интернет-магазины и интернет-аукционы, предназначенные для реализации любых товаров, работ или услуг физическим и юридическим лицам, в том числе веб-сайты магазинов, осуществляющих реализацию исключительно в интернете, так и веб-сайты обычных магазинов с возможностью оплаты онлайн.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 11 | Социальные сети                          | Категория включает веб-ресурсы, предназначенные для построения, отражения и организации контактов между людьми, организациями, государством, требующие в качестве условия участия регистрацию учетной записи пользователя.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 12 | Поиск работы                             | <p>Категория включает веб-ресурсы, предназначенные для установления контактов между работодателем и соискателем работы:</p> <ul style="list-style-type: none"> <li>Веб-сайты кадровых агентств (агентств по трудоустройству и агентств по подбору персонала).</li> <li>Веб-сайты работодателей с описанием открытых вакансий и их преимуществ.</li> <li>Независимые порталы с предложениями трудоустройства от работодателей и кадровых агентств, включая платформы для фрилансеров и биржи труда.</li> <li>Социальные сети профессионального характера, которые, помимо прочего, позволяют размещать и находить данные о специалистах, которые не находятся в активном поиске работы.</li> </ul> <p>См. также <b>Исключения</b> под таблицей.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 13 | Средства анонимного доступа              | <p>Категория включает веб-ресурсы, предоставляющие информацию или инструменты для загрузки содержимого других веб-ресурсов со следующими целями:</p> <ul style="list-style-type: none"> <li>Анонимный доступ к веб-ресурсам, в том числе к веб-ресурсам, которые преднамеренно не принимают HTTP-запросы с определенных IP-адресов или их групп (например, с IP-адресов, сгруппированных по стране происхождения).</li> <li>Обход ограничений интернет-провайдера или администратора локальной сети на доступ к веб-адресам или IP-адресам.</li> <li>Подмена IP-адреса.</li> <li>Отправка анонимных сообщений на электронную почту.</li> </ul> <p>К этой категории относятся как веб-ресурсы с содержимым, предназначенным для вышеуказанных целей (VPN, "анонимайзеры" и др.), так и веб-ресурсы, имеющие технически схожую функциональность.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 14 | Платежные системы                        | Категория включает веб-ресурсы электронных платежных систем, предоставляющие доступ к персональной учетной записи пользователя. Технически, средством проведения платежей могут служить как банковские карты любых типов (пластиковые и виртуальные, дебетовые и кредитные, локальные и международные), так и электронные деньги. Для определения категории веб-ресурса несущественно наличие таких специальных технических функций, как передача данных по протоколу SSL, использование средства проверки подлинности 3D Secure и так далее.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|    |                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21 | Запрещено полицией Японии             | Веб-ресурсы, запрещенные полицией Японии.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 22 | Программное обеспечение, аудио, видео | Категория включает веб-ресурсы, где пользователи могут загружать пакеты программного обеспечения.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 23 | Финансы, экономика                    | Категория включает веб-сайты, которые предоставляют финансовую и экономическую информацию, в том числе информацию об инвестициях, налогообложении, бухгалтерском учете, страховании, брокерской деятельности, личных финансах, пенсионном обеспечении, ипотеке и ссудах. В эту категорию также входят агентства по сбору средств и взысканию долгов.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 24 | Бизнес                                | Категория включает веб-сайты компаний, торгово-промышленных ассоциаций и промышленных групп, а также корпоративные веб-сайты. Также в нее входят веб-сайты, предлагающие корпоративные и бизнес-услуги.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 25 | Компьютерная техника, электроника     | <p>Категория включает веб-сайты, контент которых связан с техникой и бытовой электроникой:</p> <ul style="list-style-type: none"> <li>• Веб-сайты, содержащие информацию о компьютерах, их частях и аксессуарах.</li> <li>• Веб-сайты, содержащие информацию о бытовой электронике, включая, среди прочего, технические гаджеты, мобильные телефоны, телевизоры, домашние кинотеатры, аудиосистемы, DVD-плееры, игровые приставки, цифровые фотоаппараты и видеокамеры, принтеры, автомобильную электронику и устройства умного дома, подключенные к интернету.</li> <li>• Веб-сайты, на которых представлены новости технологий, инструкции и обзоры бытовой электроники.</li> <li>• Веб-сайты производителей и поставщиков описанных выше электронных устройств и оборудования в целом.</li> </ul> |
| 26 | Информационная безопасность           | <p>Категория включает веб-сайты, содержащие информацию по IT-безопасности, в том числе веб-сайты, которые предоставляют продукты и услуги безопасности для корпоративных и домашних пользователей. В эту категорию не входят страницы, содержащие информацию о способах взлома систем.</p> <p>Веб-страницы из этой категории не могут быть отнесены к другим категориям.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 27 | Азартные игры, лотереи, тотализаторы  | <p>Категория включает веб-страницы, предлагающие:</p> <ul style="list-style-type: none"> <li>• участие в азартных играх, предполагающих финансовые вложения, даже если это не является обязательным условием для доступа к сайту;</li> <li>• тотализаторы, предусматривающие денежные ставки;</li> <li>• лотереи, предусматривающие приобретение лотерейных билетов или номеров;</li> <li>• информацию, способную вызвать желание участвовать в азартных играх, тотализаторах и лотереях;</li> <li>• онлайн-игры с бесплатным участием в отдельном режиме.</li> </ul> <p>Категория может включать веб-страницы, активно рекламирующие сторонние ресурсы, попадающие в эту категорию. См. также <b>Исключения</b> под таблицей.</p>                                                                   |
| 28 | Общение в сети                        | Категория включает веб-ресурсы, позволяющие зарегистрированным и незарегистрированным пользователям отправлять персональные сообщения другим пользователям, а также публиковать общедоступные или частично доступные сообщения на соответствующих веб-ресурсах.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 29 | Спам-сайты                            | Категория включает веб-сайты, созданные специально для рассылки спама, и (или) веб-сайты, используемые в спам-письмах.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 30 | Транспорт                             | <p>Категория включает веб-сайты, посвященные моторизованным транспортным средствам:</p> <ul style="list-style-type: none"> <li>• Веб-сайты с информацией, обсуждениями и обзорами автомобилей, мотоциклов, грузовиков, лодок, самолетов и поездов.</li> <li>• Веб-сайты для покупки новых и подержанных моторизованных транспортных средств, включая запчасти и аксессуары.</li> <li>• Веб-сайты с информацией о модификации, ремонте и кастомизации транспортных средств.</li> <li>• Веб-сайты общественного транспорта</li> </ul>                                                                                                                                                                                                                                                                  |
| 31 | Искусство                             | <p>Категория включает веб-сайты, которые содержат и распространяют информацию об изобразительном и исполнительском искусстве и культурном наследии:</p> <ul style="list-style-type: none"> <li>• Веб-сайты музеев, галерей и выставок.</li> <li>• Веб-страницы, содержащие описания или изображения произведений изобразительного искусства, включая, среди прочего, живопись, скульптуру, архитектуру, литературу, фотографию и дизайн.</li> <li>• Веб-страницы, содержащие описания или изображения произведений исполнительского искусства, включая, среди прочего, театр, танцы и музыку.</li> </ul> <p>Веб-страницы из этой категории не могут быть отнесены к другим категориям.</p>                                                                                                           |
| 32 | Криптовалюты, майнинг                 | Категория включает веб-ресурсы, предлагающие услуги по покупке, продаже и хранению криптовалюты, а также консультации, связанные с криптовалютами и майнингом.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|    |                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 33 | Запрещено законодательством Бельгии         | Веб-ресурсы, запрещенные к распространению Belgian Gaming Commission.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 34 | Интернет-магазины, банки, платежные системы | Сайты интернет-магазинов, платежных систем, банков, онлайн-кошельков и бирж криптовалют.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 35 | Видеоигры                                   | <p>Категория включает веб-страницы, посвященные видеоиграм разных жанров:</p> <ul style="list-style-type: none"> <li>• Веб-сайты разработчиков, специализирующихся на видеоиграх.</li> <li>• Веб-ресурсы, посвященные обсуждению видеоигр.</li> <li>• Веб-ресурсы, предоставляющие техническую возможность участвовать в онлайн-играх, индивидуально или с другими игроками.</li> <li>• Веб-ресурсы, позволяющие играть в онлайн-игры с локальной установкой приложений или без нее ("браузерные игры").</li> <li>• Веб-ресурсы, предназначенные для рекламы, распространения и поддержки игрового программного обеспечения.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 36 | Религии, религиозные объединения            | <p>Категория включает веб-страницы с материалами об общественных движениях, объединениях и организациях, подразумевающих наличие религиозной идеологии или культа в любых проявлениях:</p> <ul style="list-style-type: none"> <li>• Веб-сайты официальных религиозных организаций разного уровня, начиная с межнациональных конфессий и заканчивая местными религиозными общинами.</li> <li>• Веб-сайты незарегистрированных религиозных объединений и сообществ, исторически появившихся в результате отделения от доминирующего религиозного объединения или сообщества.</li> <li>• Веб-сайты религиозных объединений и сообществ, появившихся независимо от традиционных религиозных течений, в том числе по инициативе конкретного основателя.</li> <li>• Веб-сайты межконфессиональных организаций, служащих для взаимодействия представителей разных традиционных религий.</li> <li>• Веб-ресурсы, содержащие подробное изображение или описание религиозных действий культов, в том числе обрядов и ритуалов, связанных с почитанием Бога, существ или предметов, наделяемых сверхъестественными свойствами.</li> </ul> <p>См. также <b>Исключения</b> под таблицей.</p> |
| 37 | Новостные ресурсы                           | <p>Категория включает веб-ресурсы, содержащие новости, формируемые СМИ или интернет-издательствами, предусматривающими добавление новостей пользователями:</p> <ul style="list-style-type: none"> <li>• Веб-сайты официальных средств массовой информации.</li> <li>• Веб-сайты, предоставляющие информационные сервисы со ссылкой на официальные источники информации.</li> <li>• Веб-сайты, предлагающие услуги новостных агрегаторов или собирающие новости из разных официальных и неофициальных источников.</li> <li>• Веб-сайты, новостной контент которых формируется самими пользователями ("сайты социальных новостей").</li> </ul> <p>Веб-страницы из этой категории не могут быть отнесены к другим категориям.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 38 | Порнография, эротика                        | <p>Категория включает:</p> <ul style="list-style-type: none"> <li>• Веб-страницы, которые содержат любые фотографии или видео с изображением половых органов людей или человекоподобных существ, а также полового акта или самоудовлетворения с участием людей или человекоподобных существ.</li> <li>• Веб-страницы, которые содержат любой текст, в том числе литературный или художественный, с описанием половых органов людей или человекоподобных существ, а также полового акта или самоудовлетворения с участием людей или человекоподобных существ.</li> <li>• В эту категорию также могут входить веб-страницы, содержащие возбуждающие эротические материалы или произведения, изображающие сексуальную жизнь человека, например произведения искусства, рассчитанные на то, чтобы вызвать сексуальное возбуждение.</li> </ul>                                                                                                                                                                                                                                                                                                                                       |
| 39 | Нудизм                                      | Категория включает веб-страницы, посвященные нудизму, в том числе веб-сайты сообществ нудистов, веб-сайты о местах отдыха для нудистов, размещающие нудистские фотографии. Также в категорию входят веб-сайты, содержащие такие фотографии.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 40 | Белье                                       | Категория включает веб-сайты производителей нижнего белья, веб-сайты, торгующие нижним бельем, а также веб-страницы, посвященные выставкам и моде, которые содержат описания нижнего белья или размещают коллекции фотографий людей в нижнем белье.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 41 | Секс-образование                            | <p>Категория включает веб-страницы, посвященные теме полового воспитания, которые не рассчитаны на то, чтобы вызывать сексуальное возбуждение, и которые содержат, среди прочего, следующие типы материалов:</p> <ul style="list-style-type: none"> <li>• Сексуальная жизнь человека, сексуальные отношения.</li> <li>• Анатомия половых органов людей или животных.</li> <li>• Сексуальная активность.</li> <li>• Половое размножение.</li> <li>• Сексуальное здоровье, советы по безопасному сексу.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|    |                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 42 | Знакомства для взрослых | Категория включает веб-сайты, предоставляющие услуги онлайн- и офлайн-знакомств для аудитории старше 18 лет с целью поиска сексуального партнера. В эту категорию также входят веб-сайты, предоставляющие эскортные услуги. В эту категорию могут входить службы знакомств, в которых профили пользователей имеют сексуальный или эротический характер.                                                                                                                                            |
| 43 | ЛГБТ+                   | Категория включает веб-сайты, посвященные тематике ЛГБТК+*.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 44 | Интим-магазины          | Категория включает веб-сайты магазинов и производителей эротических товаров и товаров для секса, в том числе презервативов, усилителей потенции, секс-аксессуаров, видеопродукции эротического содержания на физических носителях.                                                                                                                                                                                                                                                                 |
| 45 | Наркотики               | Категория включает следующие типы материалов: <ul style="list-style-type: none"> <li>• Веб-страницы, содержащие информацию о наркотических, психотропных и (или) одурманивающих веществах или их описание.</li> <li>• Веб-страницы с инструкциями по потреблению или производству таких веществ.</li> <li>• Веб-страницы с информацией о последствиях употребления наркотиков.</li> <li>• В эту категорию могут входить веб-сайты немедицинских организаций, помогающих наркозависимым.</li> </ul> |
| 46 | Алкоголь                | Категория включает: <ul style="list-style-type: none"> <li>• Веб-страницы, содержащие информацию об алкогольных продуктах или описание порядка их производства или потребления.</li> <li>• Веб-страницы, на которых рекламируется или продается алкогольная или спиртосодержащая продукция.</li> <li>• Веб-сайты производителей алкогольных напитков, таких как винодельни, пивоварни, ликеро-водочные заводы и т. д.</li> </ul>                                                                   |
| 47 | Табак                   | Категория включает: <ul style="list-style-type: none"> <li>• Веб-страницы, содержащие информацию о табачных изделиях, электронных сигаретах и аксессуарах.</li> <li>• Веб-страницы, описывающие порядок использования или потребления таких продуктов.</li> <li>• Веб-страницы, на которых рекламируются или продаются табачные изделия, а также предметы, предназначенные для их употребления.</li> </ul>                                                                                         |
| 48 | Культура, общество      | В категорию входят многие аспекты жизни общества и человека, в том числе: <ul style="list-style-type: none"> <li>• Религия, религиозные объединения.</li> <li>• Власть, политика, закон.</li> <li>• Дом и семья.</li> <li>• Новостные ресурсы.</li> <li>• Вооруженные силы.</li> <li>• Оружие.</li> <li>• Поиск работы.</li> <li>• Рестораны, еда, кафе.</li> <li>• Астрология, паранормальные явления.</li> </ul>                                                                                 |
| 49 | Власть, политика, закон | Категория включает веб-страницы правоохранительных и государственных учреждений любого уровня, независимых административных органов, политических объединений и движений, юридических бюро и юридических консультаций, а также веб-сайты с информацией о законах.<br>Веб-страницы из этой категории не могут быть отнесены к другим категориям.                                                                                                                                                    |
| 50 | Дом, семья              | Категория включает веб-страницы, содержащие информацию или рекомендации по семейному образу жизни и ведению домашнего хозяйства. Кроме того, в нее входят веб-сайты, посвященные домоводству и ремонту дома, а также страницы о домашней обстановке и декоре.                                                                                                                                                                                                                                      |
| 51 | Вооруженные силы        | Категория включает веб-страницы, посвященные военной тематике. Описания вооруженных сил, военных подразделений, вооруженных формирований, военных доктрин и милитарии. Сайты или форумы, вдохновленные вооруженными конфликтами или посвященные их обсуждению.<br>См. также <b>Исключения</b> под таблицей.                                                                                                                                                                                        |
| 52 | Рестораны, кафе, еда    | Категория включает: <ul style="list-style-type: none"> <li>• Веб-страницы ресторанов и кафе.</li> <li>• Веб-сайты с рецептами и описаниями методов приготовления пищи, включая кулинарные сообщества.</li> <li>• Веб-сайты продовольственных магазинов (работающих онлайн и офлайн).</li> </ul>                                                                                                                                                                                                    |
| 53 | Астрология, эзотерика   | Категория включает веб-страницы, содержание которых классифицируется как мистическое или эзотерическое: гороскопы, гадания, хиромантия и магия. В эту категорию также входят исследования и обсуждения, связанные с НЛО, экстрасенсорным восприятием и паранормальными явлениями.                                                                                                                                                                                                                  |

|    |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 54 | Торренты                             | Категория включает веб-торрент-ресурсы и распределенные одноранговые (peer-to-peer) сервисы обмена файлами, включая любые веб-страницы, распространяющие торрент-файлы.                                                                                                                                                                                                                                               |
| 55 | Файловые обменники                   | Категория включает веб-сайты и сервисы для обмена файлами, специально предназначенные для хранения, синхронизации и обмена файлами между пользователями.                                                                                                                                                                                                                                                              |
| 56 | Аудио, видео                         | Категория включает веб-ресурсы, распространяющие такие аудио- и видеоматериалы, включая фильмы, записи спортивных трансляций, записи концертов, песни, отрывки из фильмов, видеоролики, аудиовизуальные учебные материалы и прочее.                                                                                                                                                                                   |
| 57 | Информационные технологии            | Категория включает многие аспекты, связанные с IT-услугами и техническим оборудованием, в том числе: <ul style="list-style-type: none"> <li>• Средства анонимного доступа.</li> <li>• Поисковые машины и сервисы.</li> <li>• Хостинг.</li> <li>• Рекламные сети.</li> <li>• Интернет-сервисы.</li> <li>• Компьютерная техника, электроника.</li> <li>• Информационная безопасность.</li> <li>• Спам-сайты.</li> </ul> |
| 58 | Поисковые машины и сервисы           | Категория включает веб-сайты, которые предоставляют базу данных интернет-ресурсов со встроенной поисковой системой. Например: поиск Google, Bing®, Yahoo!.<br>Веб-страницы из этой категории не могут быть отнесены к другим категориям.                                                                                                                                                                              |
| 59 | Хостинг                              | Категория включает веб-сайты, предоставляющие услуги хостинга, регистрации доменов и поиска с помощью WHOIS.                                                                                                                                                                                                                                                                                                          |
| 60 | Реклама, тизерные сети               | Категория включает веб-сайты рекламных агентств, рекламных сетей. При этом сами баннеры не блокируются.                                                                                                                                                                                                                                                                                                               |
| 61 | Банки                                | Подкатегория включает в себя следующие типы материалов: <ul style="list-style-type: none"> <li>• Веб-сайты банков, предлагающих услуги интернет-банкинга, включая безналичные (электронные) переводы между банковскими счетами, открытие банковских вкладов, оплату услуг сторонних организаций и прочее.</li> <li>• Электронные кошельки, которые предоставляют доступ к учетной записи пользователя.</li> </ul>     |
| 62 | Недвижимость                         | Категория включает веб-страницы для аренды, продажи и покупки недвижимости.                                                                                                                                                                                                                                                                                                                                           |
| 63 | Фишинговые веб-сайты                 | Категория включает веб-страницы, представляющие угрозу потери данных, в том числе: <ul style="list-style-type: none"> <li>• Фишинг.</li> <li>• Мошенничество и другие злоумышленные действия в интернете.</li> </ul>                                                                                                                                                                                                  |
| 64 | Вредоносные веб-сайты                | URL-адреса загрузки вредоносных ресурсов или вредоносного ПО.                                                                                                                                                                                                                                                                                                                                                         |
| 65 | Самоповреждение, самоубийство        | Категория включает веб-страницы, поощряющие причинение себе вреда или самоубийство либо действия, которые представляют угрозу жизни или здоровью.                                                                                                                                                                                                                                                                     |
| 66 | Блоги                                | Категория включает веб-сайты, работающие на блог-платформах, личные блоги и веб-сайты, предоставляющие платные или бесплатные услуги по созданию и ведению блогов.                                                                                                                                                                                                                                                    |
| 67 | Сайты знакомств                      | Категория включает веб-сайты, предоставляющие услуги знакомств онлайн и офлайн.                                                                                                                                                                                                                                                                                                                                       |
| 68 | Образование                          | Категория включает веб-сайты, связанные с образованием.                                                                                                                                                                                                                                                                                                                                                               |
| 69 | Школы, университеты                  | Категория включает веб-страницы школ, университетов и других образовательных организаций. В эту подкатегорию также входят онлайн-курсы и другие образовательные веб-сервисы.<br>Веб-страницы из этой категории не могут быть отнесены к другим категориям.                                                                                                                                                            |
| 70 | Книги, писатели                      | Категория включает веб-страницы писателей, страницы о книгах и веб-сайты для обсуждения. Фан-клубы отдельных авторов и книг. Сайты издателей. Интернет-библиотеки и книжные магазины.                                                                                                                                                                                                                                 |
| 71 | Образовательные порталы, базы знаний | Категория включает сервисы онлайн-обучения и образовательные порталы по различным темам. Энциклопедии, создаваемые проверенными экспертами или пользователями.<br>Веб-страницы из этой категории не могут быть отнесены к другим категориям.                                                                                                                                                                          |
| 72 | Хобби, развлечения                   | Категория включает веб-страницы, посвященные различным увлечениям или формам отдыха. В эту категорию также входят сайты о путешествиях, музыке и домашних животных, а также сайты, связанные со зрелищами и развлечениями, включая, среди прочего, фильмы, представления, театр, телевидение, шоу-бизнес, музыку, фан-клубы, новости о знаменитостях, сплетни и комиксы.                                              |

|    |                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 73 | Охота, рыбалка            | <p>Категория включает веб-страницы, связанные с охотой и рыбалкой:</p> <ul style="list-style-type: none"> <li>• Сообщества и форумы, где обсуждают охоту и рыбалку.</li> <li>• Веб-сайты с советами и инструкциями по охоте и рыбалке.</li> <li>• Магазины, продающие рыболовное и охотничье снаряжение или оружие.</li> </ul>                                                                                                                                                                                                                                                     |
| 74 | Путешествия, поездки      | <p>Категория включает сайты, связанные с путешествиями:</p> <ul style="list-style-type: none"> <li>• Справочники и путеводители для отдельных стран и городов.</li> <li>• Услуги по бронированию отелей и билетов; отзывы об отелях и курортах, службы бронирования для туристов.</li> <li>• Туристические агентства, которые помогают с бронированием отелей и билетов на различные виды транспорта.</li> <li>• Интернет-сообщества для обсуждения различных видов туризма.</li> </ul>                                                                                            |
| 75 | ТВ, радио                 | Категория включает веб-страницы телекомпаний, онлайн-телевидения, а также веб-сайты радиокompаний и интернет-радиостанций.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 76 | Дикие и домашние животные | Категория включает веб-страницы, посвященные животным; сообщества и организации, деятельность которых посвящена животным. В эту категорию также входят инструкции по уходу за животными и онлайн-трансляции, посвященные животным.                                                                                                                                                                                                                                                                                                                                                 |
| 77 | Юмор                      | Категория включает развлекательные веб-страницы, содержащие анекдоты, мемы, юмористические рассказы или забавные видеоролики. Также она может включать сайты комедийных программ и шоу.                                                                                                                                                                                                                                                                                                                                                                                            |
| 78 | Музыка                    | <p>Категория включает:</p> <ul style="list-style-type: none"> <li>• Веб-страницы, содержащие тексты песен и ноты</li> <li>• Официальные страницы музыкальных групп, композиторов и исполнителей, содержащие песни и биографические данные.</li> <li>• Платформы для покупки билетов на музыкальные концерты.</li> <li>• Сайты музыкальных заведений: оперных театров, филармонических оркестров и т. д.</li> <li>• В эту категорию также входят платформы потоковой музыки, музыкальные телеканалы и радиоканалы.</li> </ul>                                                       |
| 79 | Красота, здоровье, спорт  | Категория включает веб-страницы, посвященные спорту, красоте и здоровью.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 80 | Спорт, спортивные игры    | Категория включает веб-страницы, посвященные любому виду спорта, истории спорта или правилам игры. В эту подкатеорию также входят сайты спортивных сообществ, команд, атлетов, болельщиков и спортивных новостей.                                                                                                                                                                                                                                                                                                                                                                  |
| 81 | Здоровье                  | Категория включает веб-страницы, посвященные здоровому образу жизни. В эту подкатеорию могут входить сайты, посвященные фитнесу, здоровому питанию и альтернативным медицинским практикам и методам.                                                                                                                                                                                                                                                                                                                                                                               |
| 82 | Мода, стиль               | Категория включает веб-страницы, посвященные моде и стилю: модельные агентства, показы и трансляции мод, а также сайты о модной и стильной одежде и обуви. Руководства по моде и стилю.                                                                                                                                                                                                                                                                                                                                                                                            |
| 83 | Медицина, фармацевтика    | <p>Категория включает:</p> <ul style="list-style-type: none"> <li>• Веб-страницы, посвященные медицине и фармацевтике в целом.</li> <li>• Веб-сайты медицинских организаций и реабилитационных центров.</li> <li>• Фармацевтические компании и страницы о лекарствах и пищевых добавках.</li> <li>• Веб-страницы с официальной информацией о профилактике инфекций, включая рекомендации по профилактике ВИЧ и рака.</li> <li>• Центр профессиональной медико-психологической помощи.</li> </ul> <p>Веб-страницы из этой категории не могут быть отнесены к другим категориям.</p> |
| 84 | Лотереи                   | Веб-страницы онлайн-лотерей и сайты, содержащие информацию о лотереях.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 85 | Казино, карточные игры    | <p>Категория включает:</p> <ul style="list-style-type: none"> <li>• Веб-сайты онлайн- и офлайн-казино.</li> <li>• Веб-сайты с информацией об азартных карточных играх и для игры в них.</li> <li>• Веб-сайты с инструкциями и советами по азартным играм.</li> <li>• Веб-сайты организаторов казино или принадлежащие производителям профессионального оборудования для казино либо содержащие информацию о нем/</li> </ul>                                                                                                                                                        |
| 86 | Онлайн-тотализаторы       | Категория включает веб-сайты онлайн- и офлайн-букмекеров, на которых можно делать ставки на результаты спортивных событий, скачек и других соревнований и (или) на другие события.                                                                                                                                                                                                                                                                                                                                                                                                 |
| 87 | Ненависть, дискриминация  | Категория включает веб-страницы, разжигающие ненависть к группам людей, поощряющие дискриминацию любого рода, пропагандирующие расизм и экстремизм или поощряющие самоповреждающее поведение или самоубийство.                                                                                                                                                                                                                                                                                                                                                                     |

|     |                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 88  | Экстремизм, расизм                                             | <p>Категория включает следующие типы материалов:</p> <ul style="list-style-type: none"> <li>• Веб-страницы, пропагандирующие экстремизм и терроризм.</li> <li>• Веб-сайты об общепризнанных террористических и экстремистских организациях.</li> <li>• Веб-страницы, пропагандирующие расизм и дискриминацию людей по признаку этнической принадлежности, убеждений или пола.</li> </ul>                                                                                                                                                                                                                                                                                                                      |
| 89  | Другие                                                         | Эта категория зарезервирована для использования в будущем. Вы можете игнорировать эту категорию.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 90  | Анорекия                                                       | <p>Категория включает веб-страницы, содержащие информацию о расстройствах пищевого поведения, поощряющие их или содержащие обсуждение их в одобрительном ключе.</p> <p>См. также <b>Исключения</b> под таблицей.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 91  | Аборты                                                         | Категория включает веб-страницы, содержащие общую информацию об абортах. Она может включать информацию от медицинских учреждений.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 92  | Детский интернет                                               | <p>Категория включает веб-страницы, предназначенные для детей: образовательные, развлекательные, коммуникационные платформы.</p> <p>Веб-страницы из этой категории не могут быть отнесены к другим категориям.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 93  | Интернет-сервисы                                               | <p>Категория включает следующие разделы:</p> <ul style="list-style-type: none"> <li>• Главные страницы глобальных и местных интернет-провайдеров.</li> <li>• Онлайн-переводчики.</li> <li>• Сервисы статистики и аналитики веб-сайтов.</li> <li>• Интернет-хостинг для разработки программного обеспечения.</li> <li>• Веб-сайты, предоставляющие веб-услуги, включая, среди прочего, компании, которые предоставляют и поддерживают сетевое оборудование, виртуализацию, оперативное программное обеспечение и системы, средства автоматизации и т. д.</li> </ul> <p>Веб-страницы из этой категории не могут быть отнесены к другим категориям.</p>                                                          |
| 94  | Запрещено законодательством Российской Федерации               | Веб-ресурсы, запрещенные законодательством Российской Федерации.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 95  | ФЗ РФ № 436                                                    | К данной категории относятся несколько категорий веб-ресурсов, как указано в статье 5 Федерального закона 436-ФЗ.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 96  | Федеральный список экстремистских материалов, действующий в РФ | Интернет-ресурсы, включенные в федеральный список экстремистских материалов Министерства юстиции РФ.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 97  | Список Роскомнадзора РФ                                        | Веб-ресурсы, включенные в Единый реестр запрещенных интернет-ресурсов Роскомнадзора.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 98  | Запрещено региональным законодательством                       | Категория включает веб-ресурсы, запрещенные законодательством на территории отдельных стран.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 99  | Непристойное содержимое                                        | Категория включает веб-страницы с текстом откровенного сексуального характера, средства массовой информации, сервисы или обсуждения, предназначенные для аудитории старше 18 лет. Такие материалы в основном представлены в явной эротической форме или их основная цель – стимулировать сексуальное возбуждение.                                                                                                                                                                                                                                                                                                                                                                                             |
| 100 | Сцены сексуального характера                                   | <p>Категория включает веб-страницы, содержащие неявные материалы о сексуальности. Такие материалы не предназначены для детской аудитории, но подростки могут ознакомиться с ними под присмотром взрослых. Например, категория включает следующие типы материалов:</p> <ul style="list-style-type: none"> <li>• Информация о сексуальной анатомии и половом размножении.</li> <li>• Противозачаточные средства, осведомленность о фертильности и планирование родов.</li> <li>• Сексуальное здоровье.</li> <li>• Советы по улучшению секса с партнером, сексуальные принадлежности и средства для повышения сексуальной активности.</li> <li>• Аборты.</li> <li>• Нагота без эротических намерений.</li> </ul> |
| 113 | Рекламные программы                                            | Веб-страницы с контентом, связанным с программным обеспечением, которое загружает или отображает нежелательную рекламу при нахождении пользователя в Сети, собирает маркетинговые данные и другую информацию без ведома пользователя или перенаправляет поисковые запросы на определенные рекламные веб-сайты.                                                                                                                                                                                                                                                                                                                                                                                                |
| 114 | Потенциально опасные программы                                 | Веб-страницы с контентом, связанным с законными программами, которые могут наносить ущерб в случае их использования злоумышленниками (с целью удаления, блокировки, изменения или копирования данных, а также нарушения производительности компьютеров или сетей).                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 122 | Узлы Tor®                                                      | Ресурс – это узел Tor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|     |                                                                 |                                                                                                                                                                                                                                                                                                                                                       |
|-----|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 123 | Динамический DNS                                                | Ресурс предоставляется службой DDNS.                                                                                                                                                                                                                                                                                                                  |
| 124 | Средства удаленного администрирования                           | На ресурсе размещается программное обеспечение для удаленного администрирования.                                                                                                                                                                                                                                                                      |
| 137 | Разрешенный веб-сайт (локальная репутационная база организации) |                                                                                                                                                                                                                                                                                                                                                       |
| 138 | Запрещенный веб-сайт (локальная репутационная база организации) |                                                                                                                                                                                                                                                                                                                                                       |
| 201 | Запрещено ассоциацией безопасного интернета Японии              | Пиратские сайты, запрещенные Ассоциацией безопасного интернета (SIA) Японии.                                                                                                                                                                                                                                                                          |
| 203 | Инструменты генеративного ИИ                                    | <p>Категория включает сайты сервисов и инструментов, основанных на алгоритмах искусственного интеллекта:</p> <ul style="list-style-type: none"> <li>• Создание оригинального контента, такого как текст, изображения, видео, музыка, код и прочее.</li> <li>• Анализ существующего контента, такого как текст, видео, аудио, код и прочее.</li> </ul> |

\*"Международное общественное движение ЛГБТ" признано экстремистским и запрещено на территории РФ.

## Исключения

Категория и подкатегории не включают:

- образовательные сайты и энциклопедии;
- сайты государственных учреждений всех уровней;
- сайты официальных средств массовой информации и газет;
- сайты научных и медицинских учреждений;
- сайты школ и университетов;
- сайты, целевой аудиторией которых являются только дети.

# Обновление стороннего программного обеспечения, используемого Kaspersky Private Security Network 4.0.3 и выше

Стабильность работы Kaspersky Private Security Network гарантируется совместно с программным обеспечением версий, используемых по умолчанию.

В случае возникновения неполадок после обновления стороннего программного обеспечения выполните возврат стороннего программного обеспечения к версиям, используемым по умолчанию.

В комплект поставки Kaspersky Private Security Network версии 4.0.3 и выше входит скрипт `upgrade_components.sh` и файл `custom_images_versions`.

Скрипт предоставляет следующие возможности:

- Обновление стороннего программного обеспечения до версий, указанных пользователем: для [стандартной конфигурации](#) и для [конфигурации с однонаправленным шлюзом](#).
- [Возврат стороннего программного обеспечения к версиям, которые Kaspersky Private Security Network использует по умолчанию](#).

## Обновление стороннего программного обеспечения

*Чтобы обновить стороннее программное обеспечение:*

1. На Управляющем узле кластера Kubernetes распакуйте архив KPSN\_install\_<версия>.tar.gz.

2. Откройте файл custom\_images\_versions из состава распакованного архива на редактирование и измените версии стороннего программного обеспечения на нужные.

Допускается редактировать репозиторий, в котором находится образ, и версию образа.

3. Обеспечьте доступность образов всех контейнеров, указанных в файле custom\_images\_versions. Для этого выполните одно из следующих действий:

- Обеспечьте доступ к интернету. В этом случае скрипт скачает необходимые контейнеры в папку upgrade\_kpsn/images.
- Добавьте образы в локальный репозиторий контейнеров, используемый Kaspersky Private Security Network.
- Поместите образы в папку upgrade\_kpsn/images.

Названия файлов должны иметь следующий формат: %imageName%-%tag%.tar.

4. Обеспечьте доступность Helm-чартов, используемых для установки контейнеров. Для этого выполните одно из следующих действий:

- Обеспечьте доступ к интернету.  
В этом случае скрипт скачает необходимые Helm-чарты в папку upgrade\_kpsn/charts.
- Выполните скрипт ./download\_external\_charts.sh, а затем скопируйте необходимые Helm-чарты из папки charts в папку upgrade\_kpsn/charts.

Названия файлов должны иметь следующий формат: %helm\_name%-%version%.tgz.

5. Запустите скрипт с помощью команды:

```
./upgrade_components.sh
```

Скрипт обновит стороннее программное обеспечение до версий, указанных в файле custom\_images\_versions.

# Обновление стороннего программного обеспечения в конфигурации с однонаправленным шлюзом

*Чтобы обновить стороннее программное обеспечение в конфигурации с однонаправленным шлюзом:*

1. [Обновите стороннее программное обеспечение](#) в открытом сегменте сети.
2. На Управляющем узле кластера Kubernetes в открытом сегменте сети скачайте необходимые образы контейнеров и Helm-чарты. Для этого запустите скрипт с помощью команды:  

```
./upgrade_components.sh --dump
```
3. На Управляющем узле кластера Kubernetes в категорированном сегменте сети распакуйте архив KPSN\_install\_<версия>.tar.gz.
4. Скопируйте папку upgrade\_kpsn вместе с её содержимым и файл custom\_images\_versions, которые находятся на Управляющем узле кластера Kubernetes в открытом сегменте сети, в папку с распакованным архивом на Управляющем узле кластера Kubernetes в категорированном сегменте сети.  
Если отобразится запрос подтверждения на замену файлов, согласитесь.
5. На Управляющем узле кластера Kubernetes в категорированном сегменте сети запустите скрипт с помощью команды:  

```
./upgrade_components.sh
```

Скрипт обновит стороннее программное обеспечение в категорированном сегменте сети до версий, указанных в файле custom\_images\_versions.

## Возврат стороннего программного обеспечения к версиям, используемым Kaspersky Private Security Network по умолчанию

*Чтобы вернуть стороннее программное обеспечение к версиям, используемым Kaspersky Private Security Network 4.0.3 по умолчанию:*

1. Убедитесь, что образы соответствующих контейнеров находятся в локальном репозитории контейнеров, используемом Kaspersky Private Security Network.
2. Если вы удалили образы контейнеров из локального репозитория контейнеров, то выполните одно из следующих действий:
  - Обеспечьте доступ к интернету.  
В этом случае скрипт скачает необходимые контейнеры в папку upgrade\_kpsn/images.
  - Добавьте образы в локальный репозиторий контейнеров, используемый Kaspersky Private Security Network.
  - Поместите образы в папку upgrade\_kpsn/images.  
Названия файлов должны иметь следующий формат: %imageName%-%tag%.tar.

3. Обеспечьте доступность Helm-чартов, используемых для установки контейнеров. Для этого выполните одно из следующих действий:

- Обеспечьте доступ к интернету.

В этом случае скрипт скачает необходимые Helm-чарты в папку `upgrade_kpsn/charts`.

- Выполните скрипт `./download_external_charts.sh`, а затем скопируйте необходимые Helm-чарты из папки `charts` в папку `upgrade_kpsn/charts`.

Названия файлов должны иметь следующий формат: `%helm_name%-%version%.tgz`.

4. Запустите скрипт с параметром `--stable`:

```
./upgrade_components.sh --stable
```

Скрипт вернет стороннее программное обеспечение к версиям, которые Kaspersky Private Security Network 4.0.3 использует по умолчанию.

Для конфигурации с однонаправленным шлюзом выполните инструкцию выше сначала в кластере в категоризованном сегменте, затем в кластере в открытом сегменте сети.

# Источники информации о программе

Страница Kaspersky Private Security Network на веб-сайте "Лаборатории Касперского"

На [странице Kaspersky Private Security Network](#) вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

# Глоссарий

## Anti-Spam

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

## Cloud Information

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

## File Reputation

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

## Gateway External

Компонент обеспечивает обновление репутационных баз компонентов Kaspersky Private Security Network в конфигурации с использованием однонаправленного шлюза. Компонент получает пакеты обновлений с репутационными базами от Kaspersky Security Network, проверяет целостность данных, упаковывает данные в файлы и отправляет файлы в категоризованный сегмент сети.

## Gateway Internal

Компонент обеспечивает обновление репутационных баз компонентов Kaspersky Private Security Network в конфигурации с использованием однонаправленного шлюза. Компонент получает файлы с данными от компонента Gateway External из открытого сегмента сети, распаковывает их, проверяет целостность данных и обеспечивает обновление репутационных баз компонентов Kaspersky Private Security Network на серверах категоризованного сегмента сети.

## Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к постоянно обновляемой базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

## 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.

## Record Management

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

## SSL

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

## URL Reputation

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

## Категории "Лаборатории Касперского"

Готовые категории данных, разработанные сотрудниками "Лаборатории Касперского". Категории могут обновляться при обновлении баз приложения. 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 приложения "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 приложениями "Лаборатории Касперского".

## Однонаправленный шлюз

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

## Открытый сегмент сети

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

## Спам

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

# Информация о стороннем коде

Информация о стороннем коде содержится в следующих файлах:

- Информация о стороннем коде, используемом серверной частью Kaspersky Private Security Network, содержится в файле `legal_notices.txt`, расположенном в директории `/usr/local/kpsn` на сервере, на котором установлена серверная часть.
- Информация о стороннем коде, используемом веб-плагином Kaspersky Private Security Network, содержится в файле `legal_notices.txt`, расположенном на сервере с установленным приложением Kaspersky Security Center Web Console в директории <Директория установки Kaspersky Security Center Web Console>/plugins/kpsn/.

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Mac – товарный знак Apple Inc.

Ubuntu, LTS являются зарегистрированными товарными знаками Canonical Ltd.

Google Chrome и Android – товарные знаки Google LLC.

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

OpenAPI – товарный знак компании The Linux Foundation.

Kubernetes является зарегистрированным товарным знаком The Linux Foundation в США и других странах.

Helm является зарегистрированным товарным знаком The Linux Foundation в США и других странах.

Bing, Microsoft, Windows и Windows Server являются товарными знаками группы компаний Microsoft.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

Red Hat Enterprise Linux – товарный знак или зарегистрированный в США и других странах товарный знак Red Hat, Inc. или дочерних компаний.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.