Kaspersky
Security Cloud для iOS

Содержание

Обзор Kaspersky Security Cloud

Kaspersky Security Cloud – это наше решение безопасности, основанное на запатентованной технологии адаптивной защиты. Решение подстраивается под ваши действия и дает персональные рекомендации о том, как лучше защитить себя и своих близких.

Например, когда вы подключаетесь к сетям Wi-Fi, совершаете покупки и вводите пароли в интернете, вам предлагается включить наиболее подходящий для этого компонент защиты.

Доступность типов подписки может варьироваться в зависимости от региона.

Функции	Бесплатная версия	Тарифный план Personal для одного iOS-устройства	Тарифный план Personal	Тарифный план Family
Количество устройств Вы можете использовать Kaspersky Security Cloud на своих смартфонах, планшетах, персональных компьютерах и Mac (недоступно в бесплатном тарифе).	до 3	1	3–5	до 20
Количество аккаунтов My Kaspersky Вы можете использовать подписку на Kaspersky Security Cloud для одного или нескольких аккаунтов.	1	1	1	до 5

Security LIVE Отображает новости безопасности от Kaspersky и обнаруживает слабые настройки операционной системы на вашем устройстве.	✓	✓	✓	✓
Kaspersky Secure Connection Устанавливает безопасное интернет-соединение с незащищенной сетью Wi-Fi с помощью технологии VPN и защищает ваши финансовые, личные и конфиденциальные данные от перехвата при передаче данных.	✓ Ограниченная версия	✓ Ограниченная версия	✓ Ограниченная версия	✓ Ограниченная версия
QR-сканер Позволяет сканировать QR-коды и получать доступ к зашифрованной них информации. При доступе выполняется проверка ссылок, содержащихся в QR-коде. Вы можете установить его из App Store. Недоступно в Японии.	✓	✗	✓	✓
Проверка аккаунтов Позволяет вам проверять ваши учетные данные на возможность утечки в публичный доступ.	✗	✓	✓	✓
Анти-Фишинг Автоматически проверяет ссылки, которые вы открываете на своем устройстве, на предмет мошенничества, вредоносных программ и других угроз кибербезопасности.	✗	✓	✓	✓

Менеджер паролей Позволяет безопасно хранить ваши персональные данные, включая пароли, паспортные данные, финансовые и медицинские записи. Синхронизирует ваши данные на всех устройствах и безопасно хранит их. Вы можете установить его из App Store.	✓ Бесплатная версия	✗	✓ Премиум-версия	✓ Премиум-версия
Защита детей Помогает вам заботиться о детях и защитить их, когда они используют приложения и просматривают сайты в интернете. Вы можете установить его из App Store.	✗	✗	✗	✓ Премиум-версия для одного аккаунта My Kaspersky
Техническая поддержка Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании приложения.	✗	✓	✓	✓

*Функция Безопасного VPN-соединения обеспечивает функциональность отдельного приложения Kaspersky Secure Connection. Удалите Kaspersky Secure Connection с мобильного устройства, чтобы приложение Kaspersky Security Cloud работало корректно. После удаления Kaspersky Secure Connection параметры приложения также будут удалены. Подписка на безлимитную версию приложения Kaspersky Secure Connection будет применена к компоненту "Безопасное VPN-соединение" внутри приложения Kaspersky Security Cloud.

Часто задаваемые вопросы

Типы подписки

Для использования Kaspersky Security Cloud ваше устройство должно быть подключено к аккаунту My Kaspersky. My Kaspersky – это единый аккаунт для управления защитой ваших устройств.

- *Пробная версия*. Перед приобретением подписки вы можете ознакомиться с бесплатной пробной версией Kaspersky Security Cloud, подходящей для использования на всех платформах. Пробная версия Kaspersky Security Cloud работает в течение короткого ознакомительного периода. После истечения срока действия пробной подписки приложение автоматически перейдет на тарифный план Free.

  Если вы хотите продолжить пользоваться всеми функциями приложения, необходимо перейти на тарифный план Personal или Family.

- *Free*. Этот тарифный план предоставляет вам возможность бесплатного использования базового набора функций защиты для 3 устройств, подключенных к одному аккаунту My Kaspersky.

- *Премиум* :

  - *Тарифный план Personal*. Этот тарифный план рассчитан на использование приложения одним человеком и не дает возможности поделиться приложением с друзьями или родственниками. Можно выбрать срок действия подписки: один месяц или один год.

  - *Тарифный план Personal для одного устройства*. Этот пакет предоставляется только на iOS-устройствах и доступен не во всех регионах. Вам будут доступны ключевые функции на вашем основном личном устройстве.

  - *Тарифный план Family.* Этот пакет дает вам право делиться правами на использование приложения с близкими вам людьми (друзьями, семьей и даже коллегами). Можно выбрать срок действия подписки: один месяц или один год.

Вы можете сравнить пакеты подписки и включенные в них функции на этой странице.

Когда вы покупаете подписку, вам может быть предложена сниженная цена на использование приложения в течение некоторого времени. Такая скидка может быть предоставлена только один раз и распространяется только на указанный период. По истечении этого периода с вас будет снята обычная плата за выбранный вами пакет.

Вы можете купить Personal и Family подписки в самом приложении. Они будут продлены автоматически. У вас также есть возможность использовать пробную версию Kaspersky Security Cloud бесплатно в течение короткого ознакомительного периода. Бесплатный ознакомительный период предоставляется только один раз.

По истечении ознакомительного периода App Store автоматически взимает плату в соответствии с выбранным вами пакетом.

> При отмене подписки в течение ознакомительного периода, вы можете продолжать пользоваться функциями приложения бесплатно только до окончания ознакомительного периода.

Управление подписками

Подписка – это приобретение права на использование приложения на определенных условиях (например, дата окончания подписки, количество устройств).

Вы можете управлять подпиской (например, купить, приостановить или возобновить ее) на странице вашего аккаунта на сайте поставщика услуг (например, аккаунта Apple). Следуйте инструкциям в App Store.

Об автоматическом продлении

Подписка может быть продлена автоматически или вручную. Автопродлеваемая подписка продлевается автоматически в конце каждого срока действия подписки, пока вы не откажитесь от нее. Подписку, обновляемую вручную, необходимо продлевать в конце каждого периода.

Если у вас не активирована функция автопродления или приложению по каким-то причинам не удалось автоматически продлить вашу подписку (истек срок действия банковской карты или банковская карта заблокирована), по окончании срока действия подписки на тарифные планы Personal или Family приложение переходит на тарифный план Free. В этом случае чтобы продолжить работу программы по тарифному плану Personal или Family, вам необходимо продлить подписку вручную на сайте "Лаборатории Касперского" или через поставщика услуг.

Приобретение подписки на Kaspersky Security Cloud не отменяет другие ваши подписки, в которые входит Kaspersky Security Cloud. Чтобы избежать дополнительных платежей, убедитесь в том, что вы отменили или отключили автопродление подписки, которая вам не нужна.

Об отмене подписки

Чтобы отказаться от подписки или отключить автопродление, выполните следующие действия:

1. Перейдите на страницу вашего аккаунта на сайте поставщика услуг.
2. Проверьте наличие активных подписок, включающих приложение, для которого вы приобретаете подписку.

   Отмените или отключите автопродление подписок, которые вам не нужны.

Вы можете купить только одну подписку на Kaspersky Security Cloud с одним Apple ID. Чтобы переключить подписку на другую учетную запись My Kaspersky, отправьте запрос в Службу технической поддержки через My Kaspersky и подробно опишите проблему.

Если у вас есть активная подписка на компонент "Безопасное VPN-соединение", вы можете использовать ее в отдельном приложении Kaspersky Secure Connection.

О Kaspersky Secure Connection

Kaspersky Secure Connection скрывает ваше настоящее местонахождение и шифрует все получаемые и отправляемые с вашего устройства данные.

Как это работает

Публичные Wi-Fi сети могут быть недостаточно защищены, например, сеть Wi-Fi может использовать уязвимый протокол шифрования или популярное для сети Wi-Fi имя (SSID). Когда вы совершаете онлайн-покупки в незащищенной сети Wi-Fi, ваши пароли и другие персональные данные могут передаваться в незашифрованном виде. Злоумышленники могут перехватить ваши конфиденциальные данные, например, узнать данные вашей банковской карты и получить доступ к деньгам.

Когда вы подключаетесь к сети Wi-Fi, приложение проверяет безопасность этой сети. Если сеть Wi-Fi незащищена, приложение предлагает включить безопасное VPN-соединение через специально выделенный виртуальный сервер. Используя виртуальный сервер, приложение отправляет и получает ваши данные по зашифрованному безопасному VPN-соединению. Этот процесс гарантирует, что никто в сети Wi-Fi не сможет перехватить ваши персональные данные.

Преимущества

Kaspersky Secure Connection имеет следующие преимущества:

- Безопасное использование платежных систем и сайтов бронирования. Никто в сети Wi-Fi не сможет перехватить данные вашей банковской карты, когда вы совершаете онлайн-платежи, бронируете номера в отелях или арендуете машину.
- Защита конфиденциальности. Посторонние не смогут определить IP-адрес вашего устройства или ваше местоположение.
- Защита персональных данных. Никто в сети Wi-Fi не сможет перехватить и прочесть ваши электронные письма и переписку в социальных сетях или чатах.

По умолчанию вы получаете ограниченную версию Kaspersky Secure Connection. Вы можете перейти на безлимитную версию.

Использование VPN может регулироваться местным законодательством. Вы можете использовать безопасное VPN-соединение только по назначению, не нарушая местное законодательство.

О предоставлении данных (ЕС, Великобритания, Бразилия, жители американского штата Калифорния)

Просмотр информации о данных, передаваемых в "Лабораторию Касперского" при использовании предыдущих версий приложения

- Kaspersky Security Cloud 2.24–2.27
- Kaspersky Security Cloud 2.140–2.23
- Kaspersky Security Cloud 2.10–2.13
- Kaspersky Security Cloud 2.9
- Kaspersky Security Cloud 2.6–2.8

Данные, передаваемые в "Лабораторию Касперского" при использовании приложения Kaspersky Security Cloud версии 2.29 и более поздних

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

Персональные данные

Вы соглашаетесь предоставлять "Лаборатории Касперского" персональные данные принимая Лицензионное соглашение, Политику конфиденциальности, Положение о маркетинге или Положение о Kaspersky Security Network. Вы можете просмотреть данные, передаваемые согласно условиям каждого юридического документа, в соответствующем юридическом документе.

Просмотр Лицензионного соглашения, Политики конфиденциальности, Положения о Kaspersky Security Network

1. Нажмите  > **О приложении** > **Юридические документы**.
2. Нажмите на название положения.

   Откроется содержание выбранного положения.

Неперсональные данные

Вы соглашаетесь передавать в "Лабораторию Касперского" неперсональные данные, принимая условия Лицензионного соглашения.

Информация о запросе обновлений:

- тип ПО
- версия ПО
- идентификатор конфигурации
- результат запроса обновлений
- код ошибки

О предоставлении данных (другие регионы)

В этом документе приведена информация о данных, передаваемых в "Лабораторию Касперского" при использовании Kaspersky Security Cloud 2.47 и более поздних версий.

Подписка и аккаунт

Типы подписки

Для использования Kaspersky Security Cloud ваше устройство должно быть подключено к аккаунту My Kaspersky. My Kaspersky – это единый аккаунт для управления защитой ваших устройств.

- *Пробная версия*. Перед приобретением подписки вы можете ознакомиться с бесплатной пробной версией Kaspersky Security Cloud, подходящей для использования на всех платформах. Пробная версия Kaspersky Security Cloud работает в течение короткого ознакомительного периода. После истечения срока действия пробной подписки приложение автоматически перейдет на тарифный план Free.

  Если вы хотите продолжить пользоваться всеми функциями приложения, необходимо перейти на тарифный план Personal или Family.

- *Free*. Этот тарифный план предоставляет вам возможность бесплатного использования базового набора функций защиты для 3 устройств, подключенных к одному аккаунту My Kaspersky.

- *Премиум* :

  - *Тарифный план Personal*. Этот тарифный план рассчитан на использование приложения одним человеком и не дает возможности поделиться приложением с друзьями или родственниками. Можно выбрать срок действия подписки: один месяц или один год.

  - *Тарифный план Personal для одного устройства*. Этот пакет предоставляется только на iOS-устройствах и доступен не во всех регионах. Вам будут доступны ключевые функции на вашем основном личном устройстве.

- *Тарифный план Family.* Этот пакет дает вам право делиться правами на использование приложения с близкими вам людьми (друзьями, семьей и даже коллегами). Можно выбрать срок действия подписки: один месяц или один год.

Вы можете сравнить пакеты подписки и включенные в них функции на этой странице.

Когда вы покупаете подписку, вам может быть предложена сниженная цена на использование приложения в течение некоторого времени. Такая скидка может быть предоставлена только один раз и распространяется только на указанный период. По истечении этого периода с вас будет снята обычная плата за выбранный вами пакет.

Вы можете купить Personal и Family подписки в самом приложении. Они будут продлены автоматически. У вас также есть возможность использовать пробную версию Kaspersky Security Cloud бесплатно в течение короткого ознакомительного периода. Бесплатный ознакомительный период предоставляется только один раз.

По истечении ознакомительного периода App Store автоматически взимает плату в соответствии с выбранным вами пакетом.

При отмене подписки в течение ознакомительного периода, вы можете продолжать пользоваться функциями приложения бесплатно только до окончания ознакомительного периода.

Активация премиум-версии приложения

Вы можете заказать подписку у поставщика услуг или в самом приложении Kaspersky Security Cloud.

Если у вас уже есть подписка, вы можете активировать премиум-версию приложения одним из следующих способов:

- Использовать подписку, найденную в вашем аккаунте My Kaspersky.

  Чтобы воспользоваться этим способом, необходимо подключить приложение к My Kaspersky.

- Ввести код активации, полученный от вашего поставщика услуг или при покупке подписки. Следуйте инструкциям на My Kaspersky.

  Если код активации был потерян или случайно удален после активации приложения, то для его восстановления обратитесь в Службу технической поддержки "Лаборатории Касперского".

Управление подписками

Подписка – это приобретение права на использование приложения на определенных условиях (например, дата окончания подписки, количество устройств).

Вы можете управлять подпиской (например, купить, приостановить или возобновить ее) на странице вашего аккаунта на сайте поставщика услуг (например, аккаунта Apple). Следуйте инструкциям в App Store.

Об автоматическом продлении

Подписка может быть продлена автоматически или вручную. Автопродлеваемая подписка продлевается автоматически в конце каждого срока действия подписки, пока вы не откажитесь от нее. Подписку, обновляемую вручную, необходимо продлевать в конце каждого периода.

Если у вас не активирована функция автопродления или приложению по каким-то причинам не удалось автоматически продлить вашу подписку (истек срок действия банковской карты или банковская карта заблокирована), по окончании срока действия подписки на тарифные планы Personal или Family приложение переходит на тарифный план Free. В этом случае чтобы продолжить работу программы по тарифному плану Personal или Family, вам необходимо продлить подписку вручную на сайте "Лаборатории Касперского" или через поставщика услуг.

Приобретение подписки на Kaspersky Security Cloud не отменяет другие ваши подписки, в которые входит Kaspersky Security Cloud. Чтобы избежать дополнительных платежей, убедитесь в том, что вы отменили или отключили автопродление подписки, которая вам не нужна.

Об отмене подписки

Чтобы отказаться от подписки или отключить автопродление, выполните следующие действия:

1. Перейдите на страницу вашего аккаунта на сайте поставщика услуг.

2. Проверьте наличие активных подписок, включающих приложение, для которого вы приобретаете подписку.

   Отмените или отключите автопродление подписок, которые вам не нужны.

Вы можете купить только одну подписку на Kaspersky Security Cloud с одним Apple ID. Чтобы переключить подписку на другую учетную запись My Kaspersky, отправьте запрос в Службу технической поддержки через My Kaspersky и подробно опишите проблему.

Если у вас есть активная подписка на компонент "Безопасное VPN-соединение", вы можете использовать ее в отдельном приложении Kaspersky Secure Connection.

Просмотр информации о подписках

Вы можете просмотреть срок действия подписок и другую информацию о подписках на приложения, которые входят в состав Kaspersky Security Cloud.

Что проверить срок действия подписки и просмотреть другую информацию, выполните следующие действия:

1. Откройте Kaspersky Security Cloud.

2. Нажмите  .

3. В верхней части меню нажмите на адрес электронной почты вашего аккаунта My Kaspersky.

   Отобразится информация о ваших подписках на установленные приложения, которые входят в состав Kaspersky Security Cloud.

Предоставление данных

О предоставлении данных (ЕС, Великобритания, Бразилия, жители американского штата Калифорния)

Просмотр информации о данных, передаваемых в "Лабораторию Касперского" при использовании предыдущих версий приложения

- Kaspersky Security Cloud 2.24–2.27
- Kaspersky Security Cloud 2.140–2.23
- Kaspersky Security Cloud 2.10–2.13
- Kaspersky Security Cloud 2.9
- Kaspersky Security Cloud 2.6–2.8

Данные, передаваемые в "Лабораторию Касперского" при использовании приложения Kaspersky Security Cloud версии 2.29 и более поздних

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

Персональные данные

Вы соглашаетесь предоставлять "Лаборатории Касперского" персональные данные принимая Лицензионное соглашение, Политику конфиденциальности, Положение о маркетинге или Положение о Kaspersky Security Network. Вы можете просмотреть данные, передаваемые согласно условиям каждого юридического документа, в соответствующем юридическом документе.

Просмотр Лицензионного соглашения, Политики конфиденциальности, Положения о Kaspersky Security Network

1. Нажмите  > **О приложении** > **Юридические документы**.
2. Нажмите на название положения.

   Откроется содержание выбранного положения.

Неперсональные данные

Вы соглашаетесь передавать в "Лабораторию Касперского" неперсональные данные, принимая условия Лицензионного соглашения.

Информация о запросе обновлений:

- тип ПО
- версия ПО
- идентификатор конфигурации
- результат запроса обновлений
- код ошибки

О предоставлении данных (другие регионы)

В этом документе приведена информация о данных, передаваемых в "Лабораторию Касперского" при использовании Kaspersky Security Cloud 2.47 и более поздних версий.

Соответствие законодательству Европейского союза

Версии Kaspersky Security Cloud, которые распространяются на территории Европейского союза, отвечают требованиям Общеевропейского регламента о персональных данных (GDPR).

Принимая условия Лицензионного соглашения и Политики конфиденциальности, вы подтверждаете, что достигли возраста, который позволяет вам установить Kaspersky Security Cloud на территории Европейского союза. После установки Kaspersky Security Cloud вам будет предложено ознакомиться и принять условия, необходимые для первоначальной настройки и использования Kaspersky Security Cloud.

Вы также можете принять два необязательных соглашения:

- Положение об обработке данных в маркетинговых целях, позволяющие "Лаборатории Касперского" предоставить вам дополнительные преимущества.
- Положение о Kaspersky Security Network, позволяющие улучшить защиту устройства и повысить эффективность работы приложения.

Если вы приняли условия этих соглашений, вы можете отменить свое решение в настройках приложения в любое время.

Просмотр дополнительных условий и положений, принятие или отказ

1. Нажмите  > **О приложении** > **Юридические документы**.
2. Нажмите на название положения.

Откроется содержание выбранного положения.

3. Ознакомьтесь с положением.

   - Если вы хотите предоставить данные для достижения заявленных в положении целей, нажмите **Включить** и примите условия положения.

   - Если вы хотите отказаться от условий положения, нажмите **Выключить**.

Согласно условиям GDPR, у вас есть определенные права в отношении ваших личных данных (подробнее читайте в разделе «Ваши права и возможности» в Политике конфиденциальности для продуктов и услуг). Согласно условиям GDPR, у вас есть право удалить все ваши персональные данные, поступившие при установке приложения, из "Лаборатории Касперского". Чтобы удалить все ваши персональные данные, поступившие от текущей установки приложения, из "Лаборатории Касперского", обратитесь в Службу технической поддержки и сообщите идентификаторы устройства и установки.

Просмотр идентификаторов устройства и установки

Нажмите  > **О приложении** > **Идентификаторы устройства и установки**.

Установка и удаление приложения

Аппаратные и программные требования

Эта справка применима для Kaspersky Security Cloud для iOS версии 2.47.0.0 и более поздних.

Для функционирования Kaspersky Security Cloud устройство должно удовлетворять следующим требованиям:

- 150 МБ свободного места в памяти устройства;

- операционная система: iOS 12.x и выше или iPadOS 13.x и выше;
- доступ в интернет.

> Kaspersky Security Cloud включает функциональность Kaspersky Secure Connection. Вы должны удалить одно из приложений, чтобы использовать другое.

Установка приложения

Чтобы установить Kaspersky Security Cloud, выполните следующие действия:

1. Перейдите в магазин App Store.
2. Найдите Kaspersky Security Cloud. Для этого нажмите **Поиск**, введите название приложения в строке поиска и нажмите **Найти**.
3. Выберите Kaspersky Security Cloud в списке результатов поиска.

   Откроется страница с информацией о Kaspersky Security Cloud.
4. На странице приложения нажмите **Загрузить**, а затем нажмите **Установить**.
5. При необходимости введите пароль от аккаунта Apple ID.

   Начнется установка приложения.

Подробнее о работе в App Store и установке приложений смотрите в руководствах пользователя для iPhone или iPad.

Как установить Kaspersky Security Cloud путем сканирования QR-кода

Чтобы получить QR-код, выполните одно из следующих действий:

- откройте Kaspersky Security Cloud для Windows и перейдите в раздел **Защита для всех устройств**.
- Откройте свой аккаунт на сайте My Kaspersky, перейдите в раздел **Загрузки**, выберите продукт, а затем нажмите **Загрузить**.

QR-код создается службами My Kaspersky и содержит важные параметры для вашей аутентификации. Не отправляйте свой QR-код кому-либо, так как это может привести к утечке данных.

Чтобы установить и войти в свой аккаунт My Kaspersky:

1. Откройте камеру или другое подобное приложение и расположите мобильное устройство так, чтобы QR-код полностью отобразился на экране устройства.

   После сканирования QR-кода вы будете перенаправлены в App Store, где сможете загрузить приложение.

2. Откройте приложение Kaspersky Security Cloud.

- Если вы хотите войти в свою учетную запись My Kaspersky автоматически (через учетную запись My Kaspersky, для которой вы создали QR-код), нажмите **Быстрый вход**.
- Если вы хотите ввести свои учетные данные вручную, нажмите **Ввести данные вручную**.

  После входа в аккаунт My Kaspersky вы можете начать использовать приложение.

Удаление приложения

Чтобы удалить Kaspersky Security Cloud, выполните следующие действия:

1. На главном экране нажмите значок **Kaspersky Security Cloud** и удерживайте его, пока значки не начнут покачиваться.
2. Нажмите  .
3. Подтвердите удаление приложения.
4. Нажмите на кнопку **Домой**.

Настройка приложения

Настройка уведомлений

Kaspersky Security Cloud показывает уведомления о различных событиях безопасности:

- Безопасное соединение
- Security LIVE

Вы можете отключить уведомления о новостях безопасности в касание  > **Настройки** > **Уведомления** > **Новости безопасности**.

Просмотр состояние защиты приложения

Чтобы просмотреть состояние защиты приложения, выполните следующие действия:

1. Откройте приложение.
2. В верхней части главного окна приложения нажмите **Подробнее**.

Отобразится окно с сообщениями от всех компонентов приложения. Вы можете нажать на сообщение, чтобы узнать детали.

Существуют три типа сообщений:

-  *Критические сообщения* информируют вас о событиях, критически важных для безопасности устройства, таких как обнаружение модифицированной прошивки.
-  *Статусные сообщения* информируют вас о том, что защита для указанной области активна.
-  *Информационные сообщения* информируют вас о событиях, потенциально важных для безопасности устройства.

Отправка статистики о расходе заряда батареи

Решение Kaspersky Security Cloud позволяет контролировать уровень заряда батареи всех устройств, на которые оформлена подписка. Вы можете просмотреть уровень заряда батареи в My Kaspersky.

Этот параметр по умолчанию включен на всех устройствах. Вы можете выключить отправку статистики о заряде батареи в настройках приложения.

Чтобы выключить отправку статистики о заряде батареи на устройстве,

Перейдите  > **Настройки** > **Отправлять уровень зарядки в My Kaspersky**.

В результате информация об уровне заряда батареи на этом устройстве будет недоступна в My Kaspersky.

Security LIVE

О компоненте Security LIVE

Компонент Security LIVE поможет вам повысить уровень защиты вашего устройства и цифрового окружения. Компонент показывает рекомендации о том, как исправить небезопасные настройки операционной системы, а также информирует о последних новостях безопасности от "Лаборатории Касперского".

О небезопасных настройках

Когда вы работаете с устройством, настройки операционной системы могут изменяться в результате ваших действий или действий приложений, которые вы запускаете. Изменение настроек операционной системы может представлять угрозу для безопасности устройства. Например, если устройстве установлена модифицированная прошивка, безопасность устройства может быть под угрозой.

Уведомления о небезопасных настройках операционной системы можно разделить на два типа:

- *Критические уведомления*. Такие настройки влияют на безопасность операционной системы и приравниваются к уязвимостям.
- *Рекомендуемые уведомления*. Такие настройки рекомендуется исправить, чтобы повысить безопасность операционной системы.

Компонент Security LIVE выполняет поиск небезопасных настроек операционной системы не реже чем раз в день. При обнаружении небезопасных настроек операционной системы, вам предлагается их исправить, чтобы восстановить безопасность операционной системы.

Информация о небезопасных настройках отображается в разделе **Security LIVE**. В разделе **Security LIVE** вы можете выполнять следующие действия:

- Просмотреть информацию о небезопасные настройках.
- Узнать, как исправить небезопасные настройки.

- Скрыть небезопасные настройки, если вы не хотите их исправлять.

О новостях безопасности

Каждый день в мире совершаются массовые кражи паролей, взломы баз данных, мошенничества в интернет-банках. Новости безопасности от "Лаборатории Касперского" предоставляют свежую информацию о таких преступлениях и помогают вам избегать ситуаций, в которых можно стать жертвой злоумышленников.

Новости безопасности отображаются в разделе **Security LIVE** вместе с другими новостями "Лаборатории Касперского". Уведомления о новостях безопасности также отображаются в панели уведомлений устройства. Если в панели уведомлений появилась новость безопасности, вы можете перейти к полному тексту новости, нажав на уведомление.

Исправление небезопасных настроек

Чтобы исправить небезопасные настройки операционной системы, выполните следующие действия:

1. Откройте главное окно приложения.
2. В разделе **Security LIVE** нажмите на настройку, которую вы хотите исправить.

   Откроется описание небезопасной настройки и рекомендованные значения.

Если вы хотите оставить небезопасную настройку без изменений и скрыть ее, нажмите **Скрыть**. Вы можете просмотреть скрытые небезопасные настройки по кнопке  в правом верхнем углу экрана.

Подборка новостей безопасности

Чтобы вы получали только актуальные для вас новости безопасности, Kaspersky Security Cloud использует информацию о вашем устройстве и приложениях, которыми вы пользуетесь. Эта информация используется только для подборки новостей, которые будут вам важны или интересны. Если вы не хотите получать эту информацию, вы можете выключить функцию.

Чтобы выключить подборку новостей безопасности, выполните следующие действия:

1. Откройте Kaspersky Security Cloud.
2. Нажмите  >  **Настройки**.
3. Выключите **Отправлять статистику для эффективного формирования маркетинговых и новостных материалов**.

Kaspersky Secure Connection

О Kaspersky Secure Connection

Kaspersky Secure Connection скрывает ваше настоящее местонахождение и шифрует все получаемые и отправляемые с вашего устройства данные.

Как это работает

Публичные Wi-Fi сети могут быть недостаточно защищены, например, сеть Wi-Fi может использовать уязвимый протокол шифрования или популярное для сети Wi-Fi имя (SSID). Когда вы совершаете онлайн-покупки в незащищенной сети Wi-Fi, ваши пароли и другие персональные данные могут передаваться в незашифрованном виде. Злоумышленники могут перехватить ваши конфиденциальные данные, например, узнать данные вашей банковской карты и получить доступ к деньгам.

Когда вы подключаетесь к сети Wi-Fi, приложение проверяет безопасность этой сети. Если сеть Wi-Fi незащищена, приложение предлагает включить безопасное VPN-соединение через специально выделенный виртуальный сервер. Используя виртуальный сервер, приложение отправляет и получает ваши данные по зашифрованному безопасному VPN-соединению. Этот процесс гарантирует, что никто в сети Wi-Fi не сможет перехватить ваши персональные данные.

Преимущества

Kaspersky Secure Connection имеет следующие преимущества:

- Безопасное использование платежных систем и сайтов бронирования. Никто в сети Wi-Fi не сможет перехватить данные вашей банковской карты, когда вы совершаете онлайн-платежи, бронируете номера в отелях или арендуете машину.
- Защита конфиденциальности. Посторонние не смогут определить IP-адрес вашего устройства или ваше местоположение.
- Защита персональных данных. Никто в сети Wi-Fi не сможет перехватить и прочесть ваши электронные письма и переписку в социальных сетях или чатах.

По умолчанию вы получаете ограниченную версию Kaspersky Secure Connection. Вы можете перейти на безлимитную версию.

Использование VPN может регулироваться местным законодательством. Вы можете использовать безопасное VPN-соединение только по назначению, не нарушая местное законодательство.

Выбор версии Kaspersky Secure Connection

Вы можете пользоваться ограниченной версией Kaspersky Secure Connection или купить подписку на безлимитную версию Kaspersky Secure Connection. Вы можете оформить или продлить подписку в приложении.

Функции	Ограниченная версия Kaspersky Secure Connection	Безлимитная версия Kaspersky Secure Connection

Защищенный трафик	Определенный объем в день	Сколько хотите
Виртуальный сервер	Выбирается автоматически	Любой из списка

Доступный объем защищенного трафика не влияет на объем интернет-трафика, предоставляемого вашим мобильным оператором. Вы можете продолжить использовать интернет после того, как достигнут лимит защищенного трафика, но ваши данные не будут защищены с помощью Kaspersky Secure Connection.

- В **ограниченной** версии безопасное VPN-соединение будет отключено при превышении лимита защищенного трафика. Приложение показывает уведомление при выключении безопасного VPN-соединения. Вы сможете заново включить безопасное VPN-соединение по истечении периода времени, указанного в главном окне приложения. Объем использованного защищенного трафика, показанный в приложении, может немного отличаться от фактически использованного объема.

- В **безлимитной** версии вам доступен неограниченный объем трафика каждый день. Ваша подписка на безлимитную версию приложения может включать либо одно, либо несколько устройств. Если ваша подписка распространяется на несколько устройств, подключите их к одному аккаунту My Kaspersky. На сайте My Kaspersky вы также можете отключить устройства от подписки.

Когда вы покупаете подписку, вам может быть предложена сниженная цена на использование приложения в течение некоторого времени. Такая скидка может быть предоставлена только один раз и распространяется только на указанный период. По истечении этого периода с вас будет снята обычная плата за выбранный вами пакет.

Включение безопасного VPN-соединения

Чтобы включить безопасное VPN-соединение:

1. Откройте Kaspersky Security Cloud.

2. В разделе **Безопасное VPN-соединение** нажмите **Включить**.

   Будет установлено безопасное VPN-соединение. Состояние безопасного VPN-соединения может изменяться во время работы приложения.

Просмотр состояния безопасного VPN-соединения и доступного трафика

Вы можете посмотреть текущее состояние безопасного VPN-соединения и проверить, защищены ли ваши данные при передаче.

В ограниченной версии вы также можете посмотреть объем защищенного трафика, доступный на сегодня. В безлимитной версии приложение не отображает данные об использовании трафика, так как вам доступен неограниченный объем защищенного трафика.

> Доступный объем защищенного трафика не влияет на объем интернет-трафика, предоставляемого вашим мобильным оператором. Вы можете продолжить использовать интернет после того, как достигнут лимит защищенного трафика, но ваши данные не будут защищены с помощью Kaspersky Secure Connection.

Чтобы просмотреть состояние безопасного VPN-соединения и доступный защищенный трафик,

Откройте главное окно приложения и перейдите в раздел **Безопасное соединение**.

Переход на безлимитную версию Kaspersky Secure Connection

Чтобы перейти на безлимитную версию:

1. Откройте Kaspersky Security Cloud.
2. В разделе **Безопасное соединение** нажмите **Открыть** > **Получить больше**.
3. Выберите подписку на месяц или на год. Для обоих видов подписки включено автопродление.

   В приложении откроется окно магазина App Store.
4. Подтвердите покупку.

Информация о подписке обновится на сайте My Kaspersky и на всех ваших устройствах, использующих Kaspersky Secure Connection.

Вы можете просмотреть детали подписки в разделе информации об учетной записи приложения.

Восстановление безлимитной версии Kaspersky Secure Connection

Если ранее вы приобретали подписку на безлимитную версию Kaspersky Secure Connection, вы можете восстановить ее. Подписка связана с вашим аккаунтом My Kaspersky.

Когда вы устанавливаете Kaspersky Secure Connection на новом устройстве или удаляете, а потом снова устанавливаете, войдите в My Kaspersky, чтобы восстановить вашу подписку.

Настройка Smart Protection

О технологии "Умная защита"

Технология Адаптивной защиты предлагает включить безопасное VPN-соединение, когда вы подключаетесь к интернету через незащищенную сеть Wi-Fi. Таким образом, вы можете безопасно вводить конфиденциальные данные, например, пользуясь общественной сетью Wi-Fi.

Вы можете настроить правила для автоматического включения безопасного VPN-соединения в сетях, которые вы часто используете.

При отсутствии интернета в незащищенной сети Wi-Fi безопасное VPN-соединение не будет включаться автоматически и приложение не будет предлагать включить безопасное VPN-соединение. При этом приложение уведомит вас об отсутствии интернета в незащищенной Wi-Fi сети.

Если вы настроили автоматическое включение безопасного VPN-соединения или нажали **Включить** для незащищенной сети Wi-Fi без подключения к интернету, приложение будет проверять наличие интернета в течение одного часа. Если интернет появится, приложение включит безопасное VPN-соединение. Если устройство отключено от сети Wi-Fi, приложение прекратит попытки включить безопасное VPN-соединение на устройстве.

Настройка безопасного VPN-соединения для неизвестных сетей Wi-Fi

При подключении к сети Kaspersky Security Cloud оценивает безопасность этой сети. Вы можете настроить автоматическое включение безопасного VPN-соединения для сетей Wi-Fi, которые признаны незащищенными.

Чтобы настроить автоматическое включение безопасного VPN-соединения для незащищенных сетей Wi-Fi, выполните следующие действия:

1. Откройте Kaspersky Security Cloud.
2. Нажмите  > **Настройки**.
3. Нажмите **Незащищенные сети Wi-Fi** и выберите одну из следующих опций:

   - **Спрашивать**. При подключении к незащищенной сети Wi-Fi отображается уведомление с предложением включить безопасное VPN-соединение.

     Разрешите Kaspersky Security Cloud показывать вам уведомления. В противном случае приложение не сможет вас предупредить и предложить установить безопасное VPN-соединение. Информацию о настройке уведомлений читайте в документации к вашей ОС.

   - **Включите Безопасное соединение**. При подключении к незащищенной сети Wi-Fi включается безопасное VPN-соединение.

- **Не реагировать**. При подключении к незащищенной сети Wi-Fi уведомление не отображается и безопасное VPN-соединение не включается.

Настройка безопасного VPN-соединения для известных сетей Wi-Fi

Если вы регулярно подключаетесь к определенной сети Wi-Fi, вы можете настроить параметры безопасного VPN-соединения для этой сети.

Чтобы настроить автоматическое включение безопасного VPN-соединения для известных сетей Wi-Fi, выполните следующие действия:

1. Откройте Kaspersky Security Cloud.
2. Нажмите  > **Настройки**.
3. Нажмите **Известные сети Wi-Fi**.

   Откроется список известных сетей Wi-Fi. Если известных сетей Wi-Fi нет, список будет пуст.
4. Выберите сеть Wi-Fi, для которой вы хотите настроить параметры безопасного VPN-соединения.
5. Выберите действие для этой сети:

   - **Использовать настройки для незащищенных сетей**. Когда устройство подключается к указанной сети Wi-Fi, используются настройки, указанные для незащищенных сетей Wi-Fi. Эти настройки применяется к известным сетям, которые признаны небезопасными. Если сеть безопасна, никаких действий не выполняется.
   - **Включите Безопасное соединение**. Когда устройство подключается к указанной сети Wi-Fi, включается безопасное VPN-соединение.
   - **Не реагировать**. Когда устройство подключается к указанной сети Wi-Fi, безопасное VPN-соединение не включается.

Разрешите Kaspersky Security Cloud показывать вам уведомления. В противном случае приложение не сможет вас предупредить и предложить установить безопасное VPN-соединение. Информацию о настройке уведомлений читайте в документации к вашей ОС.

Выбор виртуального сервера

О виртуальном сервере

Виртуальный сервер определяет ваше виртуальное местоположение в выбранной стране. Вы можете выбрать виртуальный сервер в настройках приложения. Для сайтов и приложений, которые вы открываете, вы как будто находитесь в выбранной стране.

Если вы хотите определяться в интернете как пользователь из другой страны, вы можете изменить страну, указанную в настройках виртуального сервера.

По умолчанию приложение автоматически выбирает местонахождение виртуального сервера. Как правило, выбранный виртуальный сервер обеспечивает самое быстрое соединение.

При использовании ограниченной версии нельзя выбрать виртуальный сервер. Виртуальный сервер всегда будет выбираться автоматически.

В данный момент Kaspersky Security Cloud поддерживает виртуальные сервера, которые расположены в следующих странах .

Смена виртуального сервера

Чтобы сменить виртуальный сервер:

1. Откройте Kaspersky Security Cloud.

2. Выберите раздел **Безопасное соединение**.

3. Выберите местоположение виртуального сервера.

   Если вы хотите. Чтобы приложение автоматически выбрало самый быстрый сервер, выберите опцию **Самый быстрый сервер**.

При использовании ограниченной версии нельзя выбрать виртуальный сервер. Виртуальный сервер всегда будет выбираться автоматически.

Как защитить данные, если прервалось безопасное VPN-соединение

Когда вы включаете безопасное VPN-соединение, ваши данные надежно защищены при использовании интернета. Но если безопасное VPN-соединение прервется, ваши данные не будут защищены и злоумышленники могут их заполучить. Например, когда вы гуляете по торговому центру, ваш телефон переключается с одной точки доступа Wi-Fi на другую. Каждый раз когда это происходит, Kaspersky Secure Connection нужно несколько секунд, чтобы защитить ваше новое подключение.

Чтобы ваши данные были всегда защищены, используйте функцию "Блокировка трафика для защиты" Функция "Блокировка трафика для защиты" заблокирует передачу данных через интернет, пока безопасное VPN-соединение восстанавливается. Доступ в интернет будет восстановлен, как только восстановится безопасное VPN-соединение.

По умолчанию функция "Блокировка трафика для защиты" выключена. Kaspersky Security Cloud не блокирует доступ в интернет, если безопасное VPN-соединение прервано.

Чтобы защитить ваши данные, функция "Блокировка трафика для защиты" полностью блокирует передачу данных через интернет, пока безопасное VPN-соединение не будет восстановлено.

Чтобы использовать блокировку трафика для защиты, требуется включить восстановление безопасного VPN-соединения при разрывах.

Чтобы включить блокировку трафика для защиты:

1. Откройте Kaspersky Security Cloud.
2. В главном окне приложения нажмите  .
3. В разделе **Настройки** включите опцию **Блокировка трафика для защиты**.
4. Приложение может запросить включить восстановление безопасного VPN-соединения при разрывах и предоставить необходимые разрешения. Следуйте инструкциям в интерфейсе приложения.

Приложение заблокирует доступ в интернет, если безопасное VPN-соединение прервано. Доступ в интернет будет восстановлен, как только восстановится безопасное VPN-соединение.

Просмотр статистики использования защищенного трафика на сайте My Kaspersky

Вы можете просмотреть статистику использования защищенного трафика на сайте My Kaspersky.

Чтобы просмотреть статистику:

1. Войдите на сайт My Kaspersky .
2. Перейдите в раздел **Устройства**.
3. В разделе **Устройства** выберите устройство, на котором установлено приложение Kaspersky Security Cloud.

4. Нажмите на кнопку **Статистика** в панели приложения.

   Отобразится отчет об использовании безопасного VPN-соединения за текущие сутки. Под отчетом отображается длительность VPN-соединения и виртуальный сервер.

Ограничения на использование VPN

Запрещается использование программы Kaspersky Secure Connection в следующих целях:

- Нарушение любого применимого местного, национального или международного законодательства или регулирования той страны, где находится VPN-сервер или используется программа.
- Ппричинение вреда или попытки причинения вреда несовершеннолетним любым способом.
- Использование программы недолжным образом и намеренное внедрение вредоносных компьютерных программ или любых других подобных фрагментов кода, которые являются вредоносными и / или приносят технологический ущерб.
- Проведение реверс-инжиниринга, декомпиляции, дизассемблирования, модификации, интерпретации, а также любых попыток раскрыть исходный код программы или создания производных работ.
- Получение несанкционированного доступа, вмешательство, нанесение ущерба или повреждение программы. Любое нарушение такого рода будет передано соответствующему полномочному органу исполнительной власти, и мы будем содействовать этим органам для раскрытия вашей личности. В случае такого нарушения действие ваших прав на использование программы будет немедленно прекращено;
- Загрузка, публикация, отправка по электронной почте или передача иным способом любого контента, который направлен на провокацию поведения, которое является незаконным, опасным, угрожающим, насильственным, направленным на домогательство, нечестным, дискредитирующим, аморальным, непристойным, клеветническим, посягающим на неприкосновенность частной жизни, злонамеренным или расистским, вызывающим этнические или иные конфликты, и возможно провоцирующим такое поведение.
- Выдача себя за любое другое физическое или юридическое лицо или искажение иным способом своей принадлежности к физическому или юридическому лицу в случаях, когда такая идентификация требуется или предусмотрена применимым законодательством.

- Фальсификация или манипуляция идентификаторами с целью сокрытия первоисточника любого контента, передаваемого по системам VPN.
- Загрузка, публикация, отправка по электронной почте или передача иным способом любого контента, который нарушает права на любой патент, товарный знак, коммерческую тайну, авторское право или другую интеллектуальную собственность какой-либо стороны.
- Загрузка, публикация, отправка по электронной почте или передача иным способом любых нежелательных или несанкционированных объявлений, рекламных материалов, например, "нежелательной почты", "спама", "писем счастья", или "пирамидных схем".
- Вмешательство или выведение из строя систем VPN, и /или VPN-серверов, и / или VPN-сетей, или нарушение любых требований, процедур, политик или правил сетей, подключенных к системам VPN.
- Сбор и хранение персональных данных других пользователей без их ведома.
- Распространение побуждающей к действию информации о нелегальной деятельности, а также содействие нанесению физического ущерба или травм любой группе людей или отдельным личностям или содействия любого акта насилия над животными.

"Лаборатория Касперского" не является поставщиком услуг VPN (Virtual Private Network). Если доступ к каким-либо сайтам или сервисам ограничен в регионе поставщика услуг VPN, вы не сможете получить к ним доступ с помощью программы Kaspersky Secure Connection.

Анти-Фишинг

Об Анти-Фишинге

Что такое фишинг?

Мошенники присылают вам ссылку, похожую на сайт известной компании. Они хотят, чтобы вы открыли ее и ввели свои персональные данные. Например, аккаунт Apple ID или данные банковской карты. Злоумышленники обманом получают от вас информацию, чтобы обокрасть или шантажировать вас. Этот тип мошенничества называется фишингом и, к сожалению, никакое устройство не защищено от него.

Какие сайты обычно подделывают?

Мошенники подделывают любые онлайн-сервисы, включая банки и даже Apple. Адрес ссылки может показаться вам очень похожим на официальный и отличаться только одним маленьким символом. Это отличие трудно заметить даже опытным пользователям.

Как я могу защитить свои данные?

Ответ прост — включите Анти-Фишинг. Анти-Фишинг автоматически проверяет открытые на устройстве ссылки на мошенничество, вредоносное ПО или другие киберугрозы. Если сайт опасный, то ссылка на него будет заблокирована.

Анти-Фишинг проверяет не только ссылки, которые вы открываете самостоятельно, но онлайн-активность приложений. Это может привести к блокировке некоторых функций приложений. В Японии приложение также блокирует ссылки на запрещенные сайты.

При включенном Анти-Фишинге вы сможете наблюдать за статистикой в реальном времени:

- Сколько сайтов (если конкретнее — доменов) было проверено на устройстве;
- Сколько вредоносных ссылок было заблокировано Анти-Фишингом.

Анти-Фишинг доступен только в премиум-версии приложения Kaspersky Security Cloud.

Включение Анти-Фишинг защиты

Чтобы включить Анти-Фишинг:

1. Откройте Kaspersky Security Cloud.
2. Перейдите в раздел **Анти-Фишинг** и включите функцию.

   Функция Анти-Фишинг использует технологию VPN. Поэтому когда вы включаете Анти-Фишинг, нужно разрешить приложению создать конфигурацию VPN.

Если вы выключите VPN в настройках устройства, Анти-Фишинг перестанет работать.

Когда вы включаете Анти-Фишинг, в строке состояния появляется значок VPN. Однако это не означает, что VPN включен. Чтобы включить VPN, следуйте этой инструкции.

Проверка аккаунтов

О компоненте Проверка данных

Что это такое?

Компонент **Проверка данных** проверяет ваши учетные записи на различных сайтах и предупреждает, если ваши данные попали в публичный доступ.

В бесплатной версии возможности приложения ограничены: проверка на предмет возможной утечки данных выполняется только для аккаунта My Kaspersky. Все функции приложения доступны на тарифных планах Personal и Family.

Зачем мне беспокоиться о своих данных?

Всегда есть риск, что злоумышленники взломают сайт и получат доступ к пользовательским данным. С помощью этого компонента вы можете узнать, были ли украдены данные ваших аккаунтов, а также получить рекомендации по их защите.

Как работает эта функция?

Вы можете проверять ваши аккаунты вручную или настроить автоматическую проверку аккаунтов. Kaspersky Security Cloud проверяет аккаунты по базе, предоставленной сайтом www.haveibeenpwned.com. Если при проверке будет обнаружено, что ваши данные могли попасть в публичный доступ, приложение уведомит вас об этом и покажет список сайтов, с которых могла произойти утечка данных, даты возможной утечки и категории данных, которые могли попасть в публичный доступ.

Используя Kaspersky Security Cloud, вы можете проверить на предмет возможной утечки данных не только свои, но и другие аккаунты, например, аккаунты ваших близких и друзей.

> Если вы используете тарифные планы Personal или Family, вы можете дополнительно настроить автоматическую проверку еще 50 аккаунтов кроме вашего аккаунта My Kaspersky.

При проверке аккаунтов "Лаборатория Касперского" не получает данные в открытом виде. Данные используются только для проверки и не сохраняются. При обнаружении утечки Kaspersky Security Cloud не получает доступа к самим пользовательским данным. Приложение предоставляет информацию только о категориях данных, которые могли попасть в публичный доступ.

Проверка аккаунтов

Чтобы проверить, могли ли ваши данные попасть в публичный доступ, выполните следующие действия:

1. Откройте Kaspersky Security Cloud.
2. Перейдите к разделу **Проверка учетных записей**.
3. Если вы запустили проверку в первый раз, ознакомьтесь с описанием возможностей компонента.

4. Нажмите **Проверить**.

5. В поле поиска введите ваш адрес электронной почты.

6. Нажмите **Поиск**.

   Если при проверке будет обнаружено, что ваши данные могли попасть в публичный доступ, приложение уведомит вас об этом и покажет список сайтов, с которых могла произойти утечка данных, даты возможной утечки и категории данных, которые могли попасть в публичный доступ.

   Чтобы узнать подробную информацию о возможной утечке данных и рекомендациях "Лаборатории Касперского", нажмите на веб-сайт.

7. Приложение сохраняет все проверенные аккаунты в специальный список и проверяет аккаунты из этого списка каждый день.

   При обнаружении возможной утечки вы получите уведомление.

Менеджер паролей

О компоненте Менеджер паролей

Kaspersky Password Manager защищает все ваши пароли и другую важную информацию с помощью одного мастер-пароля. Вы можете установить Kaspersky Password Manager на устройства под управлением Microsoft Windows, macOS, Android или iOS для защиты и синхронизации данных.

Работу компонента Менеджер паролей обеспечивает приложение Kaspersky Password Manager. Вам нужно установить Kaspersky Password Manager после установки основного приложения Kaspersky Security Cloud.

Версия Kaspersky Password Manager (премиум или бесплатная) зависит от вашего тарифного плана. Подробнее о тарифных планах смотрите в этом разделе.

Инструкции по использованию Kaspersky Password Manager на мобильных устройствах приведены в справке Kaspersky Password Manager https://support.kaspersky.com/help/.

Установка и запуск Kaspersky Password Manager

Чтобы загрузить и установить Kaspersky Password Manager (если приложение еще не установлено), выполните следующие действия:

1. Откройте Kaspersky Security Cloud.
2. В разделе **Kaspersky Password Manager** нажмите **Загрузить и установить**.

   Откроется страница с информацией о Kaspersky Password Manager.
3. На странице с информацией о приложении нажмите **Установить**.

   Начнется загрузка и установка приложения Kaspersky Password Manager.

Чтобы запустить приложение Kaspersky Password Manager, установленное ранее, выполните следующие действия:

1. Откройте Kaspersky Security Cloud.
2. В разделе **Kaspersky Password Manager** нажмите **Открыть**.

Откроется окно приложения Kaspersky Password Manager.

Инструкции по использованию Kaspersky Password Manager приведены в *справке Kaspersky Password Manager*.

Защита детей

О компоненте Защита детей

Посещая интернет, ваш ребенок может столкнуться с нежелательным контентом, способным навредить ему. Kaspersky Safe Kids следит за безопасностью ваших детей в интернете и в повседневной жизни. Вы решаете, что безопасно для ваших детей: какие сайты они могут посещать, как далеко уходить от дома, сколько часов проводить за компьютером или со смартфоном.

Работу компонента Защита детей обеспечивает приложение Kaspersky Safe Kids. Приложение Kaspersky Safe Kids необходимо установить после установки приложения Kaspersky Security Cloud. В пакет программ Kaspersky Security Cloud включена премиум-версия Kaspersky Safe Kids.

> Kaspersky Safe Kids доступен только в составе Kaspersky Security Cloud с тарифным планом Family.

Инструкции по использованию Kaspersky Safe Kids на мобильных устройствах приведены в справке Kaspersky Safe Kids https://support.kaspersky.com/help/.

Установка и запуск Kaspersky Safe Kids

Чтобы загрузить и установить Kaspersky Safe Kids (если приложение еще не установлено), выполните следующие действия:

1. Откройте Kaspersky Security Cloud.
2. В разделе **Kaspersky Safe Kids** нажмите **Загрузить и установить**.

   Откроется страница с информацией о Kaspersky Safe Kids.
3. На странице с информацией о приложении нажмите **Установить**.

   Начнется загрузка и установка приложения Kaspersky Safe Kids.

Чтобы запустить приложение Kaspersky Safe Kids, установленное ранее, выполните следующие действия:

1. Откройте главное окно Kaspersky Security Cloud.
2. В разделе **Kaspersky Safe Kids** нажмите **Открыть**.

Откроется окно приложения Kaspersky Safe Kids.

Инструкции по использованию Kaspersky Safe Kids приведены в *справке Kaspersky Safe Kids* .

Использование сайта My Kaspersky

О сайте My Kaspersky

My Kaspersky – это единый онлайн-ресурс для выполнения следующих задач:

- удаленного управления работой некоторых программ "Лаборатории Касперского" на устройствах;
- загрузки установочных пакетов программ "Лаборатории Касперского" на устройства;
- получения технической поддержки.

Можно войти на сайт My Kaspersky одним из следующих способов:

- использовать учетные данные других ресурсов "Лаборатории Касперского";
- создать аккаунт, если у вас его еще нет (на сайте My Kaspersky или в совместимой с сайтом программе);
- использовать учетные данные Facebook.

Для начала работы необходимо подключить ваши устройства к My Kaspersky.

Подробная информация об использовании My Kaspersky приведена в справке My Kaspersky .

Об аккаунте My Kaspersky

Аккаунт My Kaspersky требуется для входа и работы с сайтом My Kaspersky и с отдельными программами "Лаборатории Касперского".

Если у вас еще нет аккаунта My Kaspersky, вы можете создать его на сайте My Kaspersky или в совместимых с ним программах. Вы также можете использовать для входа на портал учетные данные других ресурсов "Лаборатории Касперского".

При создании аккаунта My Kaspersky вам нужно указать действующий адрес электронной почты и задать пароль. Пароль должен состоять не менее чем из 8 символов и содержать хотя бы одну цифру, одну заглавную и одну строчную латинские буквы. Пробелы не допускаются.

Если введенный пароль слишком простой или распространенный, аккаунт не будет создан.

После создания аккаунта на указанный вами адрес электронной почты будет выслано сообщение, содержащее ссылку для активации вашего аккаунта.

Активируйте аккаунт по ссылке из сообщения.

О двухэтапной проверке

Двухэтапная проверка может быть недоступна в вашем регионе. Более подробная информация приведена в справке My Kaspersky.

Двухэтапная проверка не позволит злоумышленникам войти в ваш аккаунт My Kaspersky, даже если им известен пароль. Для подтверждения вашей личности, вам по SMS будет отправлен уникальный код безопасности. Для этого используется номер телефона, указанный вами в My Kaspersky. Таким образом, для входа в аккаунт нужен и номер телефона, и пароль.

Вы можете включить двухэтапную проверку на сайте My Kaspersky. Если вы поменяли свой номер телефона, его можно обновить на сайте My Kaspersky. Если вы вошли в аккаунт на устройстве до настройки двухэтапной проверки, ничего не изменится. Более подробная информация приведена в справке My Kaspersky.

Код безопасности, отправленный вам по SMS, действителен в течение короткого периода времени. Если срок его действия истек, запросите новый код безопасности.

Если вы не получили SMS с кодом безопасности

1. Убедитесь, что мобильная сеть доступна.
2. Дождитесь появления кнопки **Запросить код повторно** в приложении.
3. Нажмите **Запросить код повторно**.

Если проблему решить не удалось, обратитесь в Службу технической поддержки.

Поделиться учетными данными My Kaspersky по ссылке

Вы можете создать персональную ссылку для установки Kaspersky Security Cloud на вашем компьютере или другом устройстве. Данные вашего аккаунта будут автоматически переданы на новое устройство.

Персональная ссылка создается службами My Kaspersky и содержит важные параметры для вашей аутентификации. Не отправляйте свою ссылку кому-либо, так как это может привести к утечке данных.

Чтобы установить Kaspersky Security Cloud на другое устройство, выполните следующие действия:

1. Откройте главное окно Kaspersky Security Cloud.

2. В разделе **Защитите все свои устройства** выберите **Подробнее**.

3. В появившемся окне нажмите **Отправить ссылку**.

   Отобразится системное окно с вариантами, как можно поделиться ссылкой.

4. Откройте ссылку на устройстве, на котором вы хотите установить Kaspersky Security Cloud.

   Теперь вы можете загрузить и установить приложение. Сразу после этого будет выполнен автоматический вход в аккаунт My Kaspersky.

Эта опция недоступна в пакете Personal для одного iOS-устройства.

Вход в My Kaspersky с помощью QR-кода

Если у вас уже есть аккаунт My Kaspersky и вы используете Kaspersky Security Cloud для Windows на своем компьютере, вы можете войти в Kaspersky Security Cloud, просканировав свой личный QR-код. Данные вашего аккаунта будут автоматически переданы на новое устройство.

QR-код создается службами My Kaspersky и содержит важные параметры для вашей аутентификации. Не отправляйте свой QR-код кому-либо, так как это может привести к утечке данных.

Как получить QR-код

1. Откройте Kaspersky Security Cloud для Windows.

2. Перейдите в раздел **Защита для всех устройств** и следуйте инструкциям в интерфейсе приложения.

Выход из аккаунта My Kaspersky

Вы можете выйти из вашего аккаунта My Kaspersky в приложении Kaspersky Security Cloud.

Вы можете пользоваться функциями приложения, только если вы вошли в свой аккаунт My Kaspersky. Когда вы выходите из аккаунта, защитные функции приложения выключаются, и устройство отключается от вашего аккаунта My Kaspersky. Когда вы снова входите в аккаунт, функции приложения возобновляют работу.

Чтобы выйти из аккаунта My Kaspersky, выполните следующие действия:

1. В меню приложения нажмите на адрес электронной почты вашего аккаунта My Kaspersky.

   Откроется окно с информацией об аккаунте.

2. Нажмите  .

3. Нажмите **Выйти из учетной записи**.

   Вы вышли из своего аккаунта My Kaspersky.

Способы получения технической поддержки

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

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки .

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

- позвонить в Службу технической поддержки по телефону;
- отправить запрос в Службу технической поддержки с сайта My Kaspersky.

Техническая поддержка предоставляется только пользователям, которые приобрели подписку на использование программы. Пользователям бесплатных версий техническая поддержка не предоставляется.

Известные проблемы

Общие проблемы

> При использовании приложения необходимо учитывать особенности устройства и руководствоваться документацией к этому устройству.

- Если на устройстве включен режим энергосбережения, следующие функции приложения будут ограничены:
  - Security LIVE
  - Kaspersky Secure Connection
- В редких случаях при активации пробной версии приложения могут возникнуть трудности. Пожалуйста, обратитесь в Службу технической поддержки "Лаборатории Касперского", если вы получили одно из следующих уведомлений: **Пробная версия недоступна** или **Не удалось получить пробную версию**.
- В редких случаях активация подписки может занять некоторое время. Чтобы активировать приложение, убедитесь, что на устройстве установлено соединение с интернетом и выполнен вход в аккаунт My Kaspersky.

- При отключении приложения от аккаунта My Kaspersky иногда приложение может предложить использовать предыдущий аккаунт My Kaspersky. Если вы выберите этот аккаунт, приложение покажет ошибку. Чтобы использовать предыдущий аккаунт, введите учетные данные вручную. Чтобы сменить аккаунт, в окне авторизации нажмите **Использовать другой аккаунт**.

- Когда приложение меняет виртуальный сервер, безопасное VPN-соединение может прерываться на короткое время. Передаваемые данные не будут защищены, пока безопасное VPN-соединение не восстановится.

- В редких случаях после покупки безлимитной версии Kaspersky Secure Connection переход приложения на безлимитную версию может занять несколько минут.

- Если ваше устройство меняет сеть при подключении к Интернету, безопасное VPN-соединение может прерываться на короткое время. Передаваемые данные не будут защищены, пока безопасное VPN-соединение не восстановится.

- Смена виртуального сервера при посещении сайтов банков, платежных систем, сайтов бронирования, социальных сетей, чатов и сайтов электронной почты может приводить к срабатыванию систем борьбы с мошенничеством (систем, предназначенных для анализа финансовых онлайн-транзакций на наличие мошеннических действий).

- VPN может использоваться только одним приложением в определенный момент времени. Если какое-либо приложение на вашем устройстве уже использует VPN, вы должны выключить VPN для этого приложения перед включением безопасного VPN-соединения в Kaspersky Security Cloud.

- Если на вашем устройстве включен режим точки доступа и интернет-соединение защищено, другие устройства, подключенные к вашей точке доступа, не смогут установить VPN-соединение с интернетом. Чтобы обеспечить интернет для других устройств, выключите безопасное VPN-соединение на своем устройстве.

- Иногда на Mac-устройствах нельзя сразу удалить Kaspersky Security Cloud.

  Как удалить Kaspersky Security Cloud

  1. Убедитесь, что функция VPN выключена.

2. Принудительно закройте приложение.

3. Удалите приложение.

Kaspersky Secure Connection

При использовании приложения необходимо учитывать особенности устройства и руководствоваться документацией к этому устройству.

- В некоторых случаях объем использованного защищенного трафика, показанный в приложении, может отличаться от фактически использованного объема защищенного трафика. Такое возможно, например, при высокоскоростном соединении.
- При подключении бесплатной версии Kaspersky Secure Connection к My Kaspersky дополнительный объем трафика добавляется к стандартному объему защищенного трафика. В некоторых случаях приложение может отображать меньший объем израсходованного защищенного трафика, чем на самом деле. Может оказаться, что вы уже использовали не только стандартный объем трафика, но и дополнительный, предоставленный вам после подключения к My Kaspersky. Тогда вы можете получить уведомление о том, что лимит защищенного трафика исчерпан, сразу после добавления дополнительного трафика.
- Когда приложение меняет виртуальный сервер, безопасное VPN-соединение может прерываться на короткое время. Передаваемые данные не будут защищены, пока безопасное VPN-соединение не восстановится.
- В редких случаях после покупки безлимитной версии Kaspersky Secure Connection переход приложения на безлимитную версию может занять несколько минут.
- Если ваше устройство меняет сеть при подключении к интернету, безопасное VPN-соединение может прерываться на короткое время. Передаваемые данные не будут защищены, пока безопасное VPN-соединение не восстановится.

- Если на вашем устройстве включен режим точки доступа и интернет-соединение защищено, другие устройства, подключенные к вашей точке доступа, не смогут установить VPN-соединение с интернетом. Чтобы обеспечить интернет для других устройств, выключите безопасное VPN-соединение на своем устройстве.

- Смена виртуального сервера при посещении сайтов банков, платежных систем, сайтов бронирования, социальных сетей, чатов и сайтов электронной почты может приводить к срабатыванию систем борьбы с мошенничеством (систем, предназначенных для анализа финансовых онлайн-транзакций на наличие мошеннических действий).

- VPN может использоваться только одним приложением в определенный момент времени. Если какое-либо приложение на вашем устройстве уже использует VPN, вы должны выключить VPN для этого приложения перед включением безопасного VPN-соединения в Kaspersky Security Cloud.

- Если вы оформили подписку с автопродлением с помощью одного аккаунта My Kaspersky, затем выполнили вход в другой аккаунт My Kaspersky, при продлении подписки на месяц будет оформлена новая неактивная подписка. Новая неактивная подписка будет принадлежать второму аккаунту My Kaspersky, в который вы выполнили вход. Так происходит потому, что онлайн-магазины не проверяют идентификатор аккаунта My Kaspersky при оформлении или продлении подписки.

- Если на вашем устройстве установлены приложения для подключения к сетям Wi-Fi, Kaspersky Security Cloud может не установить безопасное VPN-соединение для незащищенной Wi-Fi сети. Так происходит потому, что Kaspersky Security Cloud может не получить данные о подключении к сети при работе таких приложений.

- Скорость соединения может быть снижена на 50% при работающем Kaspersky Secure Connection. Мы не можем гарантировать минимальную скорость интернет-соединения.

- Если ваше устройство перешло в спящий режим, VPN- или Wi-Fi-соединение может быть потеряно из-за настроек производителя. После разблокировки устройства убедитесь, что вы все еще подключены к Wi-Fi и VPN-соединение установлено.

- Функциональность VPN может быть недоступна при подключении к IPv6-сетям. Это ограничение не касается IPv6 сетей с двумя стеками, при наличии IPv4.

- Когда вы активируете премиум-версию по ссылке или входите в систему, поделившись своими учетными данными (ссылкой или QR-кодом), Kaspersky Security Cloud проверяет буфер обмена на устройстве. Приложение обрабатывает только определенное и потенциально опасное содержимое в процессе установки. Kaspersky Security Cloud не проверяет ваши личные данные, скопированные в буфер обмена.

Если вы не можете получить доступ к сайту или веб-сервису по VPN

Некоторые сайты и веб-сервисы ограничивают доступ по VPN. Доступ к сайтам и веб-сервисам по VPN может быть запрещен по следующим причинам:

- Владельцы сайта хотят, чтобы публикуемый лицензионный контент могли просматривать только жители определенной страны, так как в разных странах действуют разные предложения и разные тарифы.

- Владельцы сайта хотят, чтобы сайт посещали только жители определенного региона. Например, лотерея разыгрывается только среди жителей определенной страны, поэтому доступ из других регионов запрещен.

- Существуют веб-сервисы, которые по законодательным причинам доступны только в определенных регионах (например, некоторые поставщики медиа-услуг или вещательные новостные компании). Эти веб-сервисы блокируют анонимайзеры и недоступны, если доступ к ним осуществляется с помощью VPN (или другого анонимайзера).

- Такие веб-сервисы не только определяют местоположение клиента, но также определяют, использует ли клиент анонимайзер. Веб-сервис блокируется при обнаружении попытки доступа к нему с помощью анонимайзера.

- Если вам не удается получить доступ к определенному сайту или веб-сервису с помощью безопасного VPN-соединения, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского". Сообщите, к какому веб-сервису вам не удается получить доступ и из какого местоположения. Служба технической поддержки "Лаборатории Касперского" постарается решить эту проблему.

Недоступность VPN в отдельных регионах

В отдельных регионах использование VPN регулируется на законодательном уровне. В настоящее время такими регионами являются:

- Республика Беларусь
- Оман
- Пакистан
- Катар
- Иран
- Саудовская Аравия
- Китай

В перечисленных странах функция VPN недоступна. "Лаборатория Касперского" старается максимально ограничить приобретение лицензии на VPN в этих регионах.

Если вы ошибочно приобрели лицензию на VPN в одном из перечисленных выше регионов, рекомендуется воспользоваться одним из следующих способов:

- Отменить вашу подписку. Дополнительную информацию см. в разделе Управление подписками.
- Обратиться в Службу технической поддержки "Лаборатории Касперского", чтобы вам помогли решить проблему.

Источники информации о приложении

Страница Kaspersky Security Cloud на сайте "Лаборатории Касперского"

На этой странице приведена общая информация о приложении, его возможностях и особенностях работы.

Страница Kaspersky Security Cloud содержит ссылку на интернет-магазин. В нем вы можете приобрести приложение или продлить право пользования приложением.

Обсуждение программ "Лаборатории Касперского" в сообществе

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и другими пользователями в сообществе .

В сообществе можно просматривать опубликованные темы, добавлять комментарии, создавать новые темы для обсуждения.

Правовая информация

Информация о стороннем коде

Информация о стороннем коде содержится в разделе **О приложении**, расположенном в меню приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apple, App Store, iPad, iPadOS, iPhone, iTunes, macOS и Safari – товарные знаки Apple Inc., зарегистрированные в США и других странах.

IOS – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и/или ее аффилированных компаний.

Android, Firebase, Google, Google AdWords, Google Analytics, Google Play – товарные знаки Google, Inc.

Бета-тестирование

О бета-версии

Бета-версии недоступны для использования на территории США.

Мы бы хотели узнать о вашем опыте использования новых функций наших мобильных продуктов и пригласить вас к участию в бета-тестировании. В бета-версии приложений вы сможете воспользоваться новыми функциями, которые еще не представлены официально.

Обратите внимание, что бета-версии могут работать менее стабильно по сравнению с основными версиями, выпущенными официально. Могут возникнуть следующие проблемы: сбои в работе приложения, ошибки при работе некоторых функций и недоступность отдельных сервисов.

Бета-версия доступна бесплатно. Однако функциональность такого приложения может быть ограничена (например, покупки становятся недоступны) Внимательно ознакомьтесь со всеми условиями и положениями Лицензионного соглашения для бета-версии.

Вы должны использовать приложение только в соответствии с функциональностью, предоставляемой установленной версией приложения. Метка оранжевого цвета рядом со значком приложения обозначает, что вы используете бета-версию приложения.

Прежде чем вы начнете бета-тестирование, внимательно ознакомьтесь с разделом Бета-версия и подписки.

Поучаствовать в бета-тестировании

Вы можете зарегистрироваться в качестве бета-тестировщика одним из следующих способов:

- Перейдите на страницу бета-версии в TestFlight и следуйте инструкциям.
- Отсканируйте QR-код и следуйте инструкциям.

Отправка отзыва

Оставляйте комментарии, рассказывайте, что вам нравится или не нравится в приложении, на странице бета-версии в TestFlight.

Завершить бета-тестирование

Перейдите на страницу бета-версии в TestFlight и следуйте инструкциям.

После завершения бета-тестирования можно загрузить основную версию приложения с App Store.

Бета-версия и подписки

Рекомендуется зарегистрировать отдельный аккаунт My Kaspersky, чтобы использовать исключительно в целях бета-тестирования.

Если вы уже приобрели лицензию, не добавляйте коды активации в учетную запись My Kaspersky, используемую для бета-тестирования. В противном случае приложение автоматически перейдет на премиум-версию, и срок действия вашей лицензии начнет истекать. Узнайте, как проверить подписки на My Kaspersky, в справке My Kaspersky .

Если вы уже используете премиум-версию, вы можете протестировать бета-версию в премиум-режиме по той же подписке. Обратите внимание, срок действия вашей лицензии не будет продлен на период бета-тестирования.