Kaspersky
Free

Содержание

Обзор приложения Kaspersky

Добро пожаловать в приложение Kaspersky! Это приложение объединяет в себе наши лучшие технологии для защиты ваших Android-устройств. Мы разработали множество функций для обеспечения вашей безопасности и приватности; кроме того, специальные инструменты в приложении помогут прокачать скорость и производительность устройства.

Приложение Kaspersky наполнено премиум-функциями и компонентами, специально разработанными для ваших устройств на Android. Здесь есть всё необходимое: от основ безопасности (анти-фишинг и поиск небезопасных настроек) и расширенных способов защиты приватности (менеджер паролей, безопасное VPN-соединение и поиск утечки данных) - до инструментов, увеличивающих скорость и производительность устройства.

Вы можете выбрать тарифный план, наиболее подходящий вам. Следующие функции доступны внутри приложения Kaspersky в рамках каждого из планов.

Функции и тарифы приложения Kaspersky

Функция	Free	Standard	Plus	Premium
Безопасность				
Антивирус	✓	✓	✓	✓
Автоматический Антивирус	✗	✓	✓	✓
Анти-Вор	✓	✓	✓	✓
Фильтр звонков	✗	✓	✓	✓
Защита чатов	✗	✓	✓	✓
Интернет-защита	✗	✓	✓	✓
Приватность				
Поиск утечки данных	✓ ограничено	✓ ограничено	✓	✓
Управление моей приватностью	✗	✗	✓	✓
Безопасное VPN-соединение	✓ ограничено	✓ ограничено	✓	✓
Блокировка приложений	✗	✓	✓	✓
Kaspersky Password Manager	✗	✗	✓	✓
Производительность				
Мои приложения	✓	✓	✓	✓
Поиск небезопасных настроек	✓	✓	✓	✓
Сеть				

Незащищенные сети Wi-Fi	✓	✓	✓	✓
Мониторинг умного дома	✗	✗	✓	✓
Другие приложения				
Kaspersky Battery Life	✓	✓	✓	✓
Безопасный QR-сканер	✓	✓	✓	✓
Дополнительные инструменты				
Количество устройств	1	до 5	до 20	до 20
Количество аккаунтов My Kaspersky	1	1	до 5	до 5
Управление подпиской	✓	✓	✓	✓
Отчеты	✓	✓	✓	✓
Поддержка				
Ответы на часто задаваемые вопросы	✓	✓	✓	✓
Рекомендации по настройке приложения	✓	✓	✓	✓
Сообщество пользователей	✓	✓	✓	✓
Премиальная техническая поддержка				
Премиальная техническая поддержка	✗	✗	✗	✓

Обратите внимание: некоторые планы могут использоваться только на одном устройстве. В рамках этих подписок вы не сможете устанавливать приложение и входить в ваш аккаунт My Kaspersky, отправляя ссылку или QR-код на другое устройство. Поделиться ссылкой или QR-кодом можно только в рамках подписок для нескольких устройств.

Если у вас есть подписка на Kaspersky Security Cloud, вы можете ее использовать и в приложении Kaspersky.

Часто задаваемые вопросы

Активация подписки на приложение Kaspersky

В настоящее время покупка подписки на приложение Kaspersky через Google Play недоступна для пользователей в России. Это связано с приостановкой платежной системы Google Play для пользователей в России. Если вы находитесь в России, вы можете приобрести годовую подписку на сайте Лаборатории Касперского. Мы уже работаем над другими вариантами приобретения подписки и будем держать вас в курсе. Спасибо, что вы с нами!

Чтобы использовать все функции приложения, вы можете подключить пробную подписку или купить и активировать подписку на приложение Kaspersky.

Для активации подписки необходимо подключение к интернету.

Если у вас уже есть подписка, вы можете активировать ее 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.

Вы можете активировать подписку при первом запуске приложения или в любое время позже.

Мы рекомендуем выполнить вход в аккаунт My Kaspersky до приобретения или продления подписки. Если вы вошли в аккаунт My Kaspersky, приложение сможет проверить, есть ли у вас уже приобретенная подписка, которую вы можете использовать для активации приложения.

Покупка подписки через Google Play

Если у вас устройство Huawei без сервисов Google Play, эта опция для вас недоступна. Вы можете активировать подписку, либо войдя в My Kaspersky, либо используя код активации.

1. Откройте приложение Kaspersky.
2. В нижнем меню нажмите **Профиль**.

3. Подключитесь к порталу My Kaspersky.

4. Нажмите **Купить или восстановить подписку**.

   Если в вашем аккаунте My Kaspersky найдена подписка, по которой можно активировать приложение, приложение Kaspersky предложит вам использовать ее для активации. Когда вы выберете найденную подписку, приложение будет автоматически активировано. Если подписка не найдена или вы предпочитаете приобрести подписку в Google Play, выберите план подписки, который вы хотите приобрести.

5. Завершите покупку в Google Play.

   После успешной активации подписки приложение сообщит, что премиум-версия активирована, и отобразит информацию о подписке.

Активация приложения по подписке, найденной в вашем аккаунте My Kaspersky

1. Откройте приложение Kaspersky.

2. В нижнем меню нажмите **Профиль**.

3. Нажмите **Купить или восстановить подписку**.

4. Нажмите **У меня есть подписка**.

5. Подключитесь к порталу My Kaspersky.

   Если в вашем аккаунте My Kaspersky найдена подписка, по которой можно активировать приложение, приложение Kaspersky предложит вам использовать ее для активации.

   После успешной активации подписки приложение сообщит, что премиум-версия активирована, и отобразит информацию о подписке.

Активация подписки с помощью кода активации

1. Откройте приложение Kaspersky.

2. В нижнем меню нажмите **Профиль**.

3. Нажмите **Купить или восстановить подписку**.

4. Нажмите **У меня есть подписка**.

5. Нажмите **Ввести код активации**.

6. Введите код активации и нажмите **Далее**.

   После успешной активации подписки приложение сообщит, что премиум-версия активирована, и отобразит информацию о подписке.

В зависимости от устройства, которое вы используете, вам могут быть предложены дополнительные возможности для активации подписки. Например, пользователи предустановленной версии приложения Kaspersky на устройствах Samsung в России также могут управлять своими подписками через аккаунт Softline.

При использовании приложения по подписке вы можете добавить другой код активации на My Kaspersky до истечения срока действия текущей подписки, ее отмены или отзыва.

На устройствах Samsung с предустановленным приложением Kaspersky вы можете приобрести подписку, продлевать ее и управлять ею через свой аккаунт Softline.

Обновление антивирусных баз

При поиске вредоносных программ приложение Kaspersky использует антивирусные базы. Антивирусные базы приложения содержат описание вредоносных программ и приложений, известных "Лаборатории Касперского" в настоящий момент, и способов их обезвреживания, а также описание других вредоносных объектов.

Для обновления антивирусных баз приложение должно быть подключено к интернету.

Чтобы запустить обновление антивирусных баз на устройстве:

1. На главном экране приложения нажмите **Все функции**.

2. Смахните вверх и нажмите **Обновить антивирусные базы**.

Если у вас есть подписка на приложение Kaspersky, вы можете настроить расписание автоматического обновления антивирусных баз.

О проверке

Вы можете запускать следующие виды проверки:

- Полная проверка

  Приложение Kaspersky проверяет все файлы на устройстве. Полная проверка помогает защитить ваши личные данные и деньги, а также обнаружить и устранить угрозы на вашем устройстве (как в установленных приложениях, так и в дистрибутивах). Полная проверка также позволяет обнаруживать рекламные приложения и приложения, которые могут быть использованы злоумышленниками для причинения вреда вашему устройству или данным на нем.

  "Лаборатория Касперского" рекомендует запускать полную проверку устройства хотя бы раз в неделю, чтобы убедиться в безопасности личных данных. Если вы не хотите запускать проверку каждый раз вручную, вы можете настроить следующие регулярные проверки:

  - Еженедельное сканирование. В бесплатной версии приложение Kaspersky автоматически проверяет все файлы на вашем устройстве не чаще одного раза в неделю. Приложение само выбирает время для этого автоматической проверки так, чтобы она не мешала вам использовать устройство. Вы не можете отключить эту проверку или запланировать время проверки. Если у вас есть подписка, вам доступна расширенная версия этой проверки в составе функции "Автоматический Антивирус".

  - Проверка всех файлов по расписанию. Если у вас есть подписка, вы можете настроить расписание, согласно которому приложение будет проверять все файлы на вашем устройстве.

- Быстрая проверка

  Приложение Kaspersky проверяет только установленные приложения. Если вы используете бесплатную версию, "Лаборатория Касперского" рекомендует запускать быструю проверку каждый раз после установки нового приложения.

  Если у вас есть подписка и вы не хотите запускать проверку вручную, вы можете настроить проверку установленных приложений по расписанию.

- Проверка отдельных папок и файлов

В связи с техническими особенностями, приложение не может проверить архивы размером 4 ГБ и более. Во время проверки приложение пропускает такие архивы. Приложение не уведомляет вас о том, что такие архивы были пропущены.

О функции "Где мое устройство"

Для предотвращения несанкционированного доступа к информации на устройстве, а также для поиска устройства в случае его потери или кражи используется функция "Где мое устройство". Можно удаленно отправлять команды на ваше устройство через My Kaspersky.

Функция "Где мое устройство" выключена по умолчанию. Чтобы удаленно отправлять команды на ваше устройство, включите на устройстве функцию "Где мое устройство". Потренируйтесь использовать отдельные функции прямо сейчас, чтобы в случае кражи или потери устройства вы смогли действовать без замешательства.

Если вы не включили функцию "Где мое устройство" до того, как ваше устройство было утеряно, вам не удастся воспользоваться ею для удаленного контроля устройства.

Через My Kaspersky можно отправлять удаленные команды, чтобы выполнять следующие действия:

- Определить местоположение устройства, заблокировать его и ввести текст, который будет отображаться на экране заблокированного устройства.
- включить на устройстве громкую сирену;
- выполнить сброс до заводских настроек на устройстве, включая очистку карты памяти;
- получить фотографии человека, который использует устройство;

  Эта функция доступна только на устройствах с фронтальной камерой.

Кроме того, с помощью функции "Где мое устройство" можно настроить выполнение следующих действий:

- Блокировку устройства, если кто-то пытается вставить в него новую SIM-карту. Для этого используйте функцию SIM-Контроль.
- Защиту от удаления приложения Kaspersky и защиту от изменения системных настроек.

Настройки функции "Где мое устройство" защищены блокировкой экрана.

Подписка и аккаунт

В настоящее время покупка подписки на приложение Kaspersky через Google Play недоступна для пользователей в России. Это связано с приостановкой платежной системы Google Play для пользователей в России. Если вы находитесь в России, вы можете приобрести годовую подписку на сайте Лаборатории Касперского. Мы уже работаем над другими вариантами приобретения подписки и будем держать вас в курсе. Спасибо, что вы с нами!

Подписка – это приобретение права на использование приложения на определенных условиях (например, дата окончания подписки, количество устройств). Подписку можно приобрести у поставщика услуг (например, Google Play, HuaweiAppGallery или в другом онлайн-магазине приложений). Вы можете управлять своей подпиской в сервисах поставщика услуг, используя свой аккаунт. Способы управления подпиской зависят от вашего провайдера. Например, по ссылкам приведены инструкции для Google Play и Huawei.

Когда вы оформляете 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 план.

Чтобы использовать приложение Kaspersky по подписке, вам необходимо войти в My Kaspersky в приложении Kaspersky и активировать подписку.

Подписка может быть продлена автоматически или вручную. Автоматически продлеваемая подписка автоматически продлевается в конце каждого периода подписки, пока вы ее не отмените (при условии своевременной предоплаты вашему поставщику услуг). Подписку, обновляемую вручную, необходимо продлевать в конце каждого периода.

После истечения срока действия подписки вам может быть предоставлен льготный период, в течение которого приложение сохранит все функции. Если подписка не продлена, по истечении льготного периода к приложению Kaspersky будут применены ограничения бесплатной версии.

> В зависимости от поставщика услуг, набор возможных действий при управлении подпиской может различаться. Кроме того, может не предоставляться льготный период, в течение которого доступно продление вашей подписки.

Чтобы отказаться от подписки, необходимо связаться с поставщиком услуг, у которого вы приобрели приложение Kaspersky.

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

Отмена подписки на приложение Kaspersky или переход на продление подписки вручную:

1. Перейдите на страницу вашем аккаунте на сайте поставщика услуг.

2. Проверьте, есть ли у вас активные подписки, которые включают в себя приложение Kaspersky.

3. Отмените или отключите автопродление подписок, которые вам не нужны.

Пробная подписка. При покупке автоматически продлеваемой подписки вы можете получить ознакомительный период, в течение которого вы можете бесплатно пользоваться всеми функциями приложения. Этот ознакомительный период предоставляется только один раз.

Если вы оформили подписку через Google Play или Huawei store, по истечении пробного периода ваш поставщик услуг автоматически спишет с вас оплату за подписку.

Если вы отмените подписку в течение пробного периода, все функции приложения будут вам доступны бесплатно только до конца пробного периода.

Пробный период и автопродление подписки могут быть недоступны на территории Индии.

Если у вас есть активная подписка на компонент "Безопасное VPN-соединение", вы можете использовать ее в отдельном приложении Kaspersky Secure Connection или в приложении Kaspersky. Вам необходимо добавить подписку в свой аккаунт My Kaspersky и войти в My Kaspersky в приложении. Подписка автоматически применится к устройству, если не достигнут лимит устройств в рамках подписки.

Просмотр информации о подписке и сроке ее действия

Вы можете просмотреть лицензионный ключ, срок подписки и другую информацию о вашей подписке.

Информация о подписке доступна для просмотра, если вы используете пробную версию или версию по подписке.

Чтобы проверить срок действия подписки и просмотреть подробную информацию:

1. Откройте приложение Kaspersky.

2. На нижней панели вкладок нажмите **Профиль**.

   Откроется окно с информацией о подписке.

Активация подписки на приложение Kaspersky

В настоящее время покупка подписки на приложение Kaspersky через Google Play недоступна для пользователей в России. Это связано с приостановкой платежной системы Google Play для пользователей в России. Если вы находитесь в России, вы можете приобрести годовую подписку на сайте Лаборатории Касперского. Мы уже работаем над другими вариантами приобретения подписки и будем держать вас в курсе. Спасибо, что вы с нами!

Чтобы использовать все функции приложения, вы можете подключить пробную подписку или купить и активировать подписку на приложение Kaspersky.

Для активации подписки необходимо подключение к интернету.

Если у вас уже есть подписка, вы можете активировать ее 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.

Вы можете активировать подписку при первом запуске приложения или в любое время позже.

Мы рекомендуем выполнить вход в аккаунт My Kaspersky до приобретения или продления подписки. Если вы вошли в аккаунт My Kaspersky, приложение сможет проверить, есть ли у вас уже приобретенная подписка, которую вы можете использовать для активации приложения.

Покупка подписки через Google Play

Если у вас устройство Huawei без сервисов Google Play, эта опция для вас недоступна. Вы можете активировать подписку, либо войдя в My Kaspersky, либо используя код активации.

1. Откройте приложение Kaspersky.
2. В нижнем меню нажмите **Профиль**.

3. Подключитесь к порталу My Kaspersky.

4. Нажмите **Купить или восстановить подписку**.

   Если в вашем аккаунте My Kaspersky найдена подписка, по которой можно активировать приложение, приложение Kaspersky предложит вам использовать ее для активации. Когда вы выберете найденную подписку, приложение будет автоматически активировано. Если подписка не найдена или вы предпочитаете приобрести подписку в Google Play, выберите план подписки, который вы хотите приобрести.

5. Завершите покупку в Google Play.

   После успешной активации подписки приложение сообщит, что премиум-версия активирована, и отобразит информацию о подписке.

Активация приложения по подписке, найденной в вашем аккаунте My Kaspersky

1. Откройте приложение Kaspersky.

2. В нижнем меню нажмите **Профиль**.

3. Нажмите **Купить или восстановить подписку**.

4. Нажмите **У меня есть подписка**.

5. Подключитесь к порталу My Kaspersky.

   Если в вашем аккаунте My Kaspersky найдена подписка, по которой можно активировать приложение, приложение Kaspersky предложит вам использовать ее для активации.

   После успешной активации подписки приложение сообщит, что премиум-версия активирована, и отобразит информацию о подписке.

Активация подписки с помощью кода активации

1. Откройте приложение Kaspersky.

2. В нижнем меню нажмите **Профиль**.

3. Нажмите **Купить или восстановить подписку**.

4. Нажмите **У меня есть подписка**.

5. Нажмите **Ввести код активации**.

6. Введите код активации и нажмите **Далее**.

   После успешной активации подписки приложение сообщит, что премиум-версия активирована, и отобразит информацию о подписке.

В зависимости от устройства, которое вы используете, вам могут быть предложены дополнительные возможности для активации подписки. Например, пользователи предустановленной версии приложения Kaspersky на устройствах Samsung в России также могут управлять своими подписками через аккаунт Softline.

При использовании приложения по подписке вы можете добавить другой код активации на My Kaspersky до истечения срока действия текущей подписки, ее отмены или отзыва.

На устройствах Samsung с предустановленным приложением Kaspersky вы можете приобрести подписку, продлевать ее и управлять ею через свой аккаунт Softline.

Вход в My Kaspersky с помощью аккаунта Google или Apple

Вам может быть доступна возможность быстрого входа в My Kaspersky с помощью аккаунта Google или Apple.

-

Вход в первый раз

Чтобы войти в My Kaspersky с помощью существующего аккаунта Google или Apple в первый раз:

1. В окне **Войдите в My Kaspersky** выберите способ авторизации и нажмите соответствующую кнопку.

2. Выберите свой регион и язык. Это влияет на способы оплаты и доступность некоторых приложений в вашем аккаунте My Kaspersky.

3. Установите флажок **Я соглашаюсь предоставить "Лаборатории Касперского" адрес своей электронной почты для получения персональных маркетинговых предложений**.

Этот шаг необязательный.

4. Нажмите **Продолжить**.

Приложение подключится к вашему аккаунту My Kaspersky.

Последующие входы

Если вы уже использовали свой аккаунт Google или Apple для входа на My Kaspersky ранее, нажмите соответствующую кнопку и следуйте инструкциям.

Приложение подключится к вашему аккаунту My Kaspersky.

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 приложение Kaspersky, просканировав свой личный QR-код. Данные вашего аккаунта будут автоматически переданы на новое устройство.

Вы можете войти в My Kaspersky с помощью QR-кода на устройствах под управлением Android 6-13.x, на которых установлен Google Play.

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.

Решение проблем с восстановлением подписки

Иногда приложение не может восстановить вашу подписку автоматически.

Удостоверьтесь, что вы вошли в My Kaspersky под аккаунтом, связанным с вашей подпиской.

Ваша подписка могла закончиться. Если это так, то вам нужно приобрести новую подписку.

Если вы уверены, что подписка не закончилась, и что вы используете нужный аккаунт My Kaspersky, пожалуйста, обратитесь в Службу технической поддержки.

Предоставление данных

Об использовании приложения на территории Европейского союза

При распространении на территории Европейского союза, приложение Kaspersky отвечает требованиям "Общеевропейского регламента о персональных данных" (General Data Protection Regulation).

Принимая условия Лицензионного соглашения и Политику конфиденциальности, вы подтверждаете, что достигли возраста, требуемого для установки приложения Kaspersky на территории Европейского союза. После установки приложение предложит вам прочитать и принять условия, необходимые для первоначальной настройки и использования приложения Kaspersky.

Вы также можете принять два необязательных положения: **Положение о Kaspersky Security Network**, необходимое для повышения скорости реакции приложения на угрозы информационной и сетевой безопасности, и **Положение об обработке данных в маркетинговых целях**, которое необходимо, чтобы "Лаборатория Касперского" имела возможность делать вам выгодные предложения. Принимая условия этих соглашений, вы можете в любой момент отклонить их в настройках приложения.

Просмотр, принятие и отклонение условий дополнительных соглашений

1. На нижней панели вкладок нажмите **Профиль** > **О программе** > **Юридическая информация**.
2. Нажмите на **Положение о Kaspersky Security Network** или **Положение об обработке данных в маркетинговых целях**.

   Откроется содержание выбранного положения.
3. Прочитайте текст соглашения:
   - Если вы хотите предоставить данные для достижения заявленных в положении целей, нажмите **Включить** и примите условия положения.
   - Если вы хотите отклонить соглашение, нажмите **Выключить**.

Кроме того, вам будет предложено принять **Положение об обработке данных с целью предоставления функциональности безопасного VPN-соединения**, которое необходимо для работы функции безопасного VPN-соединения, и **Положение об обработке данных с целью предоставления функциональности Мониторинг умного дома**, которое необходимо для работы функции "Мониторинг умного дома". Вам будет предложено принять эти положение в первый раз, когда вы откроете экраны соответствующих функций. Обратите внимание на то, что вам необходимо использовать приложение по подписке, чтобы иметь доступ к функциональности "Мониторинг умного дома".

Если вы хотите отозвать свое согласие на обработку данных, необходимых для работы функции "Мониторинг умного дома" или функции "Безопасное VPN-соединение", вы можете сделать это в любой момент.

Отзыв согласия и выключение соответствующей функции

1. В нижнем меню нажмите **Профиль** > **О приложении** > **Правовая информация**.
2. Нажмите на **Положение об обработке данных с целью предоставления функциональности Мониторинг умного дома** или на **Положение об обработке данных с целью предоставления функциональности безопасного VPN-соединения**.

   Откроется содержание выбранного положения.
3. Нажмите **Отклонить условия Положения**.
4. В появившемся окне нажмите **Отключить**.

Если вы не примете или отзовете принятие **Положения об обработке данных для обеспечения функциональности безопасного VPN-соединения**, функция "Безопасное VPN-соединение" не будет работать. Если вы не примете или отзовете принятие **Положения об обработке данных для обеспечения функциональности Мониторинг умного дома**, функция "Мониторинг умного дома" не будет работать.

Согласно условиям "Общеевропейского регламента о персональных данных" (General Data Protection Regulation), у вас есть определенные права в отношении ваших персональных данных (более подробную информацию вы можете найти в разделе "Ваши права и возможности" Политики конфиденциальности для продуктов и сервисов). Вы имеете право удалить все свои личные данные, предоставленные при загрузке приложения "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

> В нижнем меню нажмите **Профиль** > **О приложении** > **Идентификаторы устройства и установки**.

Кроме того, если вы хотите воспользоваться своим правом на удаление уже отправленных данных, вы можете запросить удаление, напрямую связавшись с нами через форму на сайте: https://support.kaspersky.com/general/privacy .

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

Просмотр информации о данных, предоставленных "Лаборатории Касперского" при использовании предыдущих версий приложения.

- Приложение Kaspersky 11.89.X.XXX
- Приложение Kaspersky 11.85.X.XXX
- Приложение Kaspersky 11.84.X.XXX
- Приложение Kaspersky 11.64.X.XXX
- Приложение Kaspersky 11.54.X.XXX
- Приложение Kaspersky 11.41.4.XXXX
- Приложение Kaspersky 11.34.4.2569
- Приложение Kaspersky 11.27.4.2246
- Приложение Kaspersky 11.23.4.2043
- Приложение Kaspersky 11.20.4.1026
- Приложение Kaspersky 11.20.4.806

Данные, передаваемые в "Лабораторию Касперского" приложением Kaspersky, начиная с версии 11.96.X.XXX

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

Мы используем персональные и неперсональные данные.

Персональные данные

Вы можете просмотреть данные, передаваемые в рамках Лицензионного соглашения, Политики конфиденциальности, Положения об обработке данных в маркетинговых целях и Положения о Kaspersky Security Network, в соответствующем юридическом документе.

Просмотр юридического документа

1. В нижнем меню приложения нажмите **Профиль**.
2. Нажмите **О приложении** > **Юридическая информация**.

   Откроется окно **Правовая информация**.
3. Нажмите на название документа, который вы хотите просмотреть.

Неперсональные данные

Мы используем следующие неперсональные данные для поддержания основных функций программного обеспечения:

- тип контрольной суммы обрабатываемого объекта;
- идентификатор компонента ПО;
- формат данных в запросе к инфраструктуре Правообладателя;
- адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP);
- номер порта;
- название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя;
- тип сработавшей записи в антивирусных базах ПО;
- идентификатор сработавшей записи в антивирусных базах ПО;

- временная метка сработавшей записи в антивирусных базах ПО;
- публичный ключ, которым подписан APK-файл;
- контрольная сумма сертификата, которым подписан APK-файл;
- имя пакета приложения;
- имя магазина, из которого приложение устанавливается;
- временная метка цифрового сертификата;
- URL сайта;
- IP-адрес сайта;
- порт;
- хеш сертификата сайта;
- содержимое сертификата;
- тип юридического соглашения, принятого пользователем при использовании ПО;
- версия юридического соглашения, принятая пользователем при использовании ПО;
- признак, указывающий, принял ли пользователь условия юридического соглашения при использовании ПО;
- дата и время, когда пользователь принял условия Соглашения при использовании Программного обеспечения;
- идентификатор продукта в сервисе KSN;
- полная версия приложения;
- идентификатор конфигурационного файла, используемого в продукте;
- результат обращения к сервису Discovery;
- код ошибки обращения к сервису Discovery.

Для целей основной функциональности следующие данные будут предоставляться и обрабатываться в сервисе Firebase:

- идентификатор программы в Firebase;

- имя пакета приложения;
- версию операционной системы.
- версия пакета SDK Firebase;
- дата и время установки Программного обеспечения
- уникальная сопоставленная ссылка, которую сервер должен проверить до выполнения соответствия отпечатков (по мере необходимости);
- код языка устройства;
- код языка устройства, полученный путем выполнения кода JavaScript в WebView;
- модель устройства;
- высота экрана устройства
- ширина экрана устройства
- настройка часового пояса устройства

Передача данных в сервисы Firebase осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Firebase доступна по адресу https://www.firebase.com/terms/privacy-policy.html .

Для целей функциональности QR сканер следующие данные будут предоставляться и обрабатываться в сервисе Huawei:

- имя пакета приложения;
- идентификатор программного обеспечения;
- версия компонента ПО;
- идентификатор сервиса;
- имя API;
- результат действий, выполненных ПО;
- общая длительность обработки запроса
- дата и время начала запроса;
- идентификатор запроса

- код мобильного оператора;
- информация о радио- и интернет-соединении;
- код страны;
- модель устройства;
- идентификатор прошивки;
- версию операционной системы.
- тип устройства;
- общее количество выполненных запросов;
- количество программных ошибок;
- количество обработанных объектов;
- формат обрабатываемого объекта;
- идентификатор действия, выполняемого пользователем в ПО;
- минимальная длительность обработки объекта;
- максимальная длительность обработки объекта;
- гистограмма обработанного изображения;
- идентификатор алгоритма обработки объекта;
- длина строки, используемой для создания штрих-кода;
- ширина создаваемого штрих-кода;
- высота создаваемого штрих-кода;
- ширина созданного штрих-кода;
- высота созданного штрих-кода;
- цвет, поля и цвет фона создаваемого штрих-кода.

Передача данных в сервис Huawei осуществляется по защищенному каналу. Обработка данных происходит согласно политике сервиса Huawei и доступна по адресу: https://consumer.huawei.com/ru/privacy/privacy-policy/ .

О предоставлении данных (другие регионы)

Просмотр информации о данных, предоставленных "Лаборатории Касперского" при использовании предыдущих версий приложения.

- Приложение Kaspersky 11.89.X.XXX
- Приложение Kaspersky 11.85.X.XXX
- Приложение Kaspersky 11.84.X.XXX
- Приложение Kaspersky 11.64.X.XXX
- Приложение Kaspersky 11.54.X.XXX
- Приложение Kaspersky 11.41.4.XXXX
- Приложение Kaspersky 11.34.4.2569
- Приложение Kaspersky 11.27.4.2246
- Приложение Kaspersky 11.23.4.2043
- Приложение Kaspersky 11.20.4.1026
- Приложение Kaspersky 11.20.4.806

Данные, передаваемые в "Лабораторию Касперского" приложением Kaspersky, начиная с версии 11.96.X.XXX

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

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. В нижнем меню нажмите **Профиль** > **О приложении** > **Правовая информация**.
2. Нажмите на название положения.

   Откроется содержание выбранного положения.

Кроме того, принимая условия Лицензионного соглашения, вы соглашаетесь предоставить «Лаборатории Касперского» следующие данные:

- тип контрольной суммы обрабатываемого объекта;
- идентификатор компонента ПО;
- формат данных в запросе к инфраструктуре Правообладателя;
- адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP);
- номер порта;
- название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя;
- тип сработавшей записи в антивирусных базах ПО;
- идентификатор сработавшей записи в антивирусных базах ПО;
- временная метка сработавшей записи в антивирусных базах ПО;
- публичный ключ, которым подписан APK-файл;
- контрольная сумма сертификата, которым подписан APK-файл;
- имя пакета приложения;
- имя магазина, из которого приложение устанавливается;
- временная метка цифрового сертификата;
- URL сайта;
- IP-адрес сайта;
- порт;

- хеш сертификата сайта;
- содержимое сертификата;
- тип юридического соглашения, принятого пользователем при использовании ПО;
- версия юридического соглашения, принятая пользователем при использовании ПО;
- признак, указывающий, принял ли пользователь условия юридического соглашения при использовании ПО;
- дата и время, когда пользователь принял условия Соглашения при использовании Программного обеспечения;
- идентификатор продукта в сервисе KSN;
- полная версия приложения;
- идентификатор конфигурационного файла, используемого в продукте;
- результат обращения к сервису Discovery;
- код ошибки обращения к сервису Discovery.

Для обеспечения основной функциональности ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Huawei Push Kit:

- идентификатор AAID (анонимный идентификатор приложения);
- push-токен;
- статус подписки на тему;
- запись о доставке сообщения;
- запись о токене ПО;
- журнал отображения, нажатия и закрытия;
- кеш содержимого сообщения.

Передача данных в сервис Huawei Push Kit осуществляется по защищенному каналу. Доступ к информации и ее защита регулируется соответствующими условиями использования сервиса Huawei Push Kit.

Для обеспечения основной функциональности ПО, предустановленного на устройства Samsung, следующие данные будут автоматически отправляться на регулярной основе в сервис SbS Softline:

- уникальный идентификатор установки;
- идентификатор устройства;
- идентификатор товарной позиции ПО;
- модель устройства;
- поставщик услуг.

Передача данных в сервис SbS Softline осуществляется по защищенному каналу. Доступ к информации и защита информации регулируются политикой конфиденциальности. Вы можете найти и прочитать ее полное содержание по адресу http://samsung.enaza.ru/get_av/privacypolicy

Функциональность Управление моей приватностью позволяет Вам изменять настройки конфиденциальности в сторонних сервисах. Для предоставления этой функциональности следующие данные будут автоматически отправляться на регулярной основе в выбираемый вами сервис для их обработки для заявленных целей:

- логин;
- пароль учётной записи пользователя в онлайн-сервисе.
- -

Передача данных в выбираемый вами сервис осуществляется по защищенному каналу. Информация об условиях обработки данных в выбираемом вами сервисе содержится в Политике конфиденциальности соответствующего сервиса.

Доступность сервиса зависит от региона и версии используемого ПО и может отличаться по регионам и версиям.

Для целей основной функциональности следующие данные будут предоставляться и обрабатываться в сервисе Firebase:

- идентификатор программы в Firebase;
- имя пакета приложения;
- версию операционной системы.

- версия пакета SDK Firebase;
- дата и время установки Программного обеспечения
- уникальная сопоставленная ссылка, которую сервер должен проверить до выполнения соответствия отпечатков (по мере необходимости);
- код языка устройства;
- код языка устройства, полученный путем выполнения кода JavaScript в WebView;
- модель устройства;
- высота экрана устройства
- ширина экрана устройства
- настройка часового пояса устройства

Передача данных в сервисы Firebase осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Firebase доступна по адресу https://www.firebase.com/terms/privacy-policy.html .

Для целей функциональности QR сканер следующие данные будут предоставляться и обрабатываться в сервисе Huawei:

- имя пакета приложения;
- идентификатор программного обеспечения;
- версия компонента ПО;
- идентификатор сервиса;
- имя API;
- результат действий, выполненных ПО;
- общая длительность обработки запроса
- дата и время начала запроса;
- идентификатор запроса
- код мобильного оператора;
- информация о радио- и интернет-соединении;

- код страны;
- модель устройства;
- идентификатор прошивки;
- версию операционной системы.
- тип устройства;
- общее количество выполненных запросов;
- количество программных ошибок;
- количество обработанных объектов;
- формат обрабатываемого объекта;
- идентификатор действия, выполняемого пользователем в ПО;
- минимальная длительность обработки объекта;
- максимальная длительность обработки объекта;
- гистограмма обработанного изображения;
- идентификатор алгоритма обработки объекта;
- длина строки, используемой для создания штрих-кода;
- ширина создаваемого штрих-кода;
- высота создаваемого штрих-кода;
- ширина созданного штрих-кода;
- высота созданного штрих-кода;
- цвет, поля и цвет фона создаваемого штрих-кода.

Передача данных в сервис Huawei осуществляется по защищенному каналу. Обработка данных происходит согласно политике сервиса Huawei и доступна по адресу: https://consumer.huawei.com/ru/privacy/privacy-policy/ .

Установка и удаление приложения

Аппаратные и программные требования

Эта справка применима для приложения Kaspersky версии 11.90.X.XXXX и более поздних.

Для функционирования приложения Kaspersky устройство должно удовлетворять следующим требованиям:

- смартфон или планшет с разрешением экрана от 320x480 пикселей;
- 120 МБ свободного места в основной памяти устройства;
- операционная система: Android 6.0-13.x.

  Если на устройстве с операционной системой Android установлена модифицированная прошивка, это повышает риск взлома устройства и кражи или повреждения ваших данных.

  На устройствах с операционной системой Android 6, если вы выбрали Расширенный режим в настройках Постоянной защиты, приложение не обнаруживает вредоносные приложения при копировании их в файловую систему устройства. Это происходит из-за известной проблемы на Android 6. Последующее сканирование файловой системы успешно обнаруживает вредоносные приложения.

- архитектура процессора Intel Atom x86 или ARMv7 и более поздние версии.

Приложение должно быть установлено в основную память устройства.

Установка приложения

Вы можете установить приложение Kaspersky с помощью сервисов Google, Huawei или других провайдеров.

Чтобы установить приложение Kaspersky:

1. Откройте сайт или магазин приложений на вашем устройстве.
2. Выберите приложение Kaspersky.
3. Откройте страницу приложения и нажмите **Установить**. Начнется установка приложения.

4. Откройте приложение и ознакомьтесь со списком прав, которые нужны приложению Kaspersky.

   - Если вы согласны предоставить приложению эти права, перейдите в Настройки устройства, найдите приложение Kaspersky и разрешите доступ к управлению всеми файлами.

   - Если вы отказываетесь предоставить приложению необходимые разрешения, удалите приложение.

Если на вашем ваше устройстве установлен Android 13, вам будет предложено предоставить приложению разрешение на отображение уведомлений. Если вы не дадите приложению Kaspersky это разрешение, оно не сможет уведомлять вас о статусе вашей защиты, состоянии лицензии и других изменениях, связанных с приложением.

Некоторые шаги могут отличаться в зависимости от магазина приложений, который вы используете.

Для получения дополнительной информации об использовании Google Play перейдите в Справочный центр Google Play . Для получения дополнительной информации об использовании AppGallery перейдите на сайт поддержки AppGallery .

Обновление приложения

Чтобы пользоваться самой стабильной версией приложения и его функциями вам нужно регулярно обновлять приложение Kaspersky. Вы можете включить автообновление в магазинах приложений или скачивать обновления вручную.

Чтобы узнать, как включить автоматическое обновление или обновить приложение вручную в Google Play, ознакомьтесь с этой статьей Справочного центра Google Play .

Чтобы узнать, как включить автоматическое обновление или обновить приложение вручную в HUAWEI AppGallery, ознакомьтесь с этой статьей Службы поддержки Huawei .

Удаление приложения

Мы рекомендуем использовать меню приложения Kaspersky для удаления приложения.

Чтобы удалить приложение Kaspersky:

1. Откройте приложение Kaspersky.

2. На нижней панели вкладок нажмите **Профиль** > **Настройки** > **Удалить приложение**.
3. В окне **Удаление Kaspersky** нажмите **Далее**.
4. Если нужно, введите секретный код приложения.

   Приложение запрашивает секретный код, если в настройках функции "Где мое устройство" установлен флажок **Защита от удаления**.
5. Подтвердите удаление приложения Kaspersky.

Приложение Kaspersky будет удалено с устройства.

Если вы включили функцию "Где мое устройство", приложение Kaspersky будет назначено администратором устройства. Перед удалением приложения Kaspersky через список приложений или Google Play необходимо отключить для него права администратора.

Как отключить права администратора для приложения

1. Откройте **Настройки** > **Безопасность** > **Администраторы устройства** (названия разделов могут отличаться в зависимости от версии Android).
2. Снимите флажок для приложения Kaspersky.
3. Нажмите **Отключить** .
4. Введите свой секретный код, если приложение запрашивает его.

   Права администратора будут отключены. В зависимости от используемой версии Android устройство будет заблокировано с помощью секретного кода, графического ключа или отпечатка пальца.

Если вы используете на своем устройстве предустановленную версию приложения Kaspersky, вы можете отключить приложение в системных настройках устройства. Приложение Kaspersky по-прежнему будет установлено на вашем устройстве, но не начнет работать, пока вы не включите его.

Проверка

Запуск полной проверки

"Лаборатория Касперского" рекомендует запускать полную проверку устройства хотя бы раз в неделю, чтобы убедиться в безопасности личных данных.

Чтобы запустить полную проверку,

На главном экране приложения Kaspersky нажмите **Проверка устройства** > **Полная проверка**.

Запуск быстрой проверки

С помощью быстрой проверки вы можете проверить только установленные приложения. Если вы используете бесплатную версию, "Лаборатория Касперского" рекомендует запускать быструю проверку каждый раз после установки нового приложения.

Чтобы выполнить быструю проверку,

На главном экране приложения Kaspersky нажмите **Проверка устройства** > **Быстрая проверка**.

О проверке

Вы можете запускать следующие виды проверки:

- Полная проверка

  Приложение Kaspersky проверяет все файлы на устройстве. Полная проверка помогает защитить ваши личные данные и деньги, а также обнаружить и устранить угрозы на вашем устройстве (как в установленных приложениях, так и в дистрибутивах). Полная проверка также позволяет обнаруживать рекламные приложения и приложения, которые могут быть использованы злоумышленниками для причинения вреда вашему устройству или данным на нем.

  "Лаборатория Касперского" рекомендует запускать полную проверку устройства хотя бы раз в неделю, чтобы убедиться в безопасности личных данных. Если вы не хотите запускать проверку каждый раз вручную, вы можете настроить следующие регулярные проверки:

  - Еженедельное сканирование. В бесплатной версии приложение Kaspersky автоматически проверяет все файлы на вашем устройстве не чаще одного раза в неделю. Приложение само выбирает время для этого автоматической проверки так, чтобы она не мешала вам использовать устройство. Вы не можете отключить эту проверку или запланировать время проверки. Если у вас есть подписка, вам доступна расширенная версия этой проверки в составе функции "Автоматический Антивирус".

  - Проверка всех файлов по расписанию. Если у вас есть подписка, вы можете настроить расписание, согласно которому приложение будет проверять все файлы

на вашем устройстве.

- Быстрая проверка

  Приложение Kaspersky проверяет только установленные приложения. Если вы используете бесплатную версию, "Лаборатория Касперского" рекомендует запускать быструю проверку каждый раз после установки нового приложения.

  Если у вас есть подписка и вы не хотите запускать проверку вручную, вы можете настроить проверку установленных приложений по расписанию.

- Проверка отдельных папок и файлов

В связи с техническими особенностями, приложение не может проверить архивы размером 4 ГБ и более. Во время проверки приложение пропускает такие архивы. Приложение не уведомляет вас о том, что такие архивы были пропущены.

Запуск проверки папок и файлов

Вы можете проверить файл или папку во внутренней памяти устройства или на карте памяти.

Чтобы проверить папку или файл, выполните следующие действия:

1. На главном экране приложения Kaspersky нажмите **Проверка устройства** > **Выборочная проверка**.
2. Выберите папку или файл для проверки.
3. Нажмите  для запуска проверки.

Настройка еженедельной "умной" проверки

Эта функция является функцией с ранним доступом.

Еженедельная "умная" проверка всех файлов включена по умолчанию, так что вам не нужно ее настраивать. Если вы не хотите, чтобы на вашем устройстве регулярно выполнялась "умная" проверка, вы можете отключить эту функцию.

Чтобы отключить еженедельную "умную" проверку:

1. На главном экране приложения Kaspersky нажмите **Автоматический Антивирус**.

2. Нажмите **Ручная и регулярная проверки**.

3. Снимите флажок **Еженедельная "умная" проверка**.

   Еженедельная "умная" проверка больше не будет выполняться.

Обновление антивирусных баз

При поиске вредоносных программ приложение Kaspersky использует антивирусные базы. Антивирусные базы приложения содержат описание вредоносных программ и приложений, известных "Лаборатории Касперского" в настоящий момент, и способов их обезвреживания, а также описание других вредоносных объектов.

Для обновления антивирусных баз приложение должно быть подключено к интернету.

Чтобы запустить обновление антивирусных баз на устройстве:

1. На главном экране приложения нажмите **Все функции**.

2. Смахните вверх и нажмите **Обновить антивирусные базы**.

Если у вас есть подписка на приложение Kaspersky, вы можете настроить расписание автоматического обновления антивирусных баз.

Где мое устройство

Для предотвращения несанкционированного доступа к информации на устройстве, а также для поиска устройства в случае его потери или кражи используется функция "Где мое устройство". Можно удаленно отправлять команды на ваше устройство через My Kaspersky.

Функция "Где мое устройство" выключена по умолчанию. Чтобы удаленно отправлять команды на ваше устройство, включите на устройстве функцию "Где мое устройство". Потренируйтесь использовать отдельные функции прямо сейчас, чтобы в случае кражи или потери устройства вы смогли действовать без замешательства.

Если вы не включили функцию "Где мое устройство" до того, как ваше устройство было утеряно, вам не удастся воспользоваться ею для удаленного контроля устройства.

Через My Kaspersky можно отправлять удаленные команды, чтобы выполнять следующие действия:

- Определить местоположение устройства, заблокировать его и ввести текст, который будет отображаться на экране заблокированного устройства.
- включить на устройстве громкую сирену;
- выполнить сброс до заводских настроек на устройстве, включая очистку карты памяти;
- получить фотографии человека, который использует устройство;

  Эта функция доступна только на устройствах с фронтальной камерой.

Кроме того, с помощью функции "Где мое устройство" можно настроить выполнение следующих действий:

- Блокировку устройства, если кто-то пытается вставить в него новую SIM-карту. Для этого используйте функцию SIM-Контроль.
- Защиту от удаления приложения Kaspersky и защиту от изменения системных настроек.

Настройки функции "Где мое устройство" защищены блокировкой экрана.

Включение функции "Где мое устройство"

Чтобы начать пользоваться функцией "Где мое устройство", выполните следующие действия:

1. На нижней панели вкладок приложения «Лаборатория Касперского» нажмите **Все функции**.
2. Нажмите **Где мое устройство**

   Откроются настройки функции.
3. Нажмите **Включить** .
4. Просмотрите описание функции и нажмите **Далее**.
5. Предоставьте приложению необходимые разрешения. Эти разрешения необходимы для защиты устройства в случае кражи или потери.
6. Войдите в ваш аккаунт My Kaspersky, если вы не сделали этого ранее.
7. Настройте блокировку экрана, если вы не сделали этого ранее при настройке **Блокировки приложений**.

8. Предоставьте приложению расширенные права путем активации Администратора устройства. Эти разрешения необходимы для выполнения команд функции "Где мое устройство" на устройстве, если оно было потеряно или украдено.

   a. На экране с информацией о расширенных правах нажмите **Далее**.

   b. Ознакомьтесь с описанием разрешений администратора устройства.

   c. Нажмите **Активировать права администратора для устройства**.

   Некоторые шаги могут различаться в зависимости от модели устройства и версии операционной системы.

9. Нажмите **Готово**.

Чтобы гарантировано получать координаты устройства при выполнении команды Найти и заблокировать, перейдите к системным параметрам и разрешите использование Wi-Fi, Bluetooth и мобильных сетей для определения местоположения устройства. Использование только GPS и датчиков устройства может оказаться недостаточным для определения местоположения устройства.

Функция "Где мое устройство" настроена. Основные функции включены. При необходимости включите дополнительные функции защиты: SIM-Контроль и защиту от удаления.

Если вы не хотите использовать отдельные функции компонента, на главном экране функции "Где мое устройство" нажмите на панель с названием функции и выключите ее с помощью переключателя.

Что делать, если устройство потеряно или украдено

Если ваше мобильное устройство потеряно или украдено, вы можете заблокировать устройство и попробовать определить его местоположение. Если устройство вернуть невозможно, то вы можете удалить с него все данные. Вы можете управлять устройством, отправляя на него команды с My Kaspersky.

Вы можете удаленно управлять потерянным или украденным мобильным устройством с помощью My Kaspersky, только если на устройстве работает приложение Kaspersky. Вам нужно настроить функцию Анти-Вор в приложении, чтобы защитить ваше устройство. Чтобы мобильное устройство получило команду, это устройство должно быть включено и подключено к интернету. Для получения дополнительной информации, пожалуйста, обратитесь к справке программы на Kaspersky Online Help.

Чтобы отправить команду на ваше мобильное устройство, выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Нажмите на интересующее вас устройство.

   Откроется окно управления мобильным устройством.
3. Нажмите на кнопку **<название команды>**.
4. Подтвердите действие.

   Состояние и результат выполнения команды показывается в разделе **История Анти-Вора**.

Вы можете отправить на мобильное устройство следующие команды:

- **Блокирование и Поиск**

  Эта команда позволяет заблокировать мобильное устройство и найти его с помощью систем GPS и GSM. Координаты местоположения мобильного устройства будут отображены на карте в блоке результатов. Дополнительно координаты местоположения будут отправлены на адрес электронной почты, указанный в параметрах аккаунта. Также вы можете оставить текст, который будет отображаться на экране заблокированного мобильного устройства.

- **Сирена**

  Эта команда позволяет включить сирену на потерянном мобильном устройстве даже с выключенным звуком и заблокировать его. Также вы можете оставить текст, который будет отображаться на экране заблокированного мобильного устройства.

- **Тайное фото**

  Эта команда позволяет сделать фотографии человека, который в данный момент использует ваше мобильное устройство, и заблокировать это устройство. Вы можете получить фотографии только с мобильного устройства с фронтальной камерой. На остальных устройствах эта команда не будет выполнена. Полученные фотографии вы можете просмотреть в разделе результатов. Также вы можете оставить текст, который будет отображаться на экране заблокированного мобильного устройства.

[Как просмотреть полученные фото](#)

Чтобы просмотреть полученные фото, выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Нажмите на интересующее вас устройство.

   Откроется окно управления мобильным устройством.
3. Перейдите на закладку **Анти-Вор**.
4. В разделе **История Анти-Вора** откройте подраздел **Тайное фото**.

   Отображаются состояние и результат выполнения команды.

Тайные фотографии недоступны в Германии по местному законодательству. Устройство только блокируется.

- **Удаление всех данных**

  Эта команда позволяет удалить все данные, хранящиеся на вашем мобильном устройстве. Мобильное устройство будет возвращено к заводским настройкам.

Если вы отправите команду на удаление всех данных на мобильное устройство, то после выполнения команды приложение Kaspersky также будет удалено. Мобильное устройство не сможет принимать последующие дистанционные команды.

Настройка SIM-Контроль

Чтобы настроить параметры функции SIM-Контроль:

1. На нижней панели вкладок приложения «Лаборатория Касперского» нажмите **Все функции**.
2. Нажмите **Где мое устройство**.
3. Разблокируйте доступ к функции с помощью секретного кода, графического ключа или отпечатка пальца.
4. В разделе **Дополнительная защита** нажмите **SIM-Контроль**.

5. Включите эту функцию, чтобы разрешить удаленную блокировку устройства при замене SIM-карты.

Защита от удаления приложения

Вы можете защитить приложение Kaspersky от несанкционированного удаления с устройства. Если ваше устройство было украдено, злоумышленники не смогут удалить приложение Kaspersky и помешать вам воспользоваться функцией "Где мое устройство".

Изменение некоторых системных настроек нарушает работу функций защиты в приложении Kaspersky. При включении защиты от удаления эти системные параметры также становятся защищенными от изменения. При попытке их изменения происходит блокировка устройства. Вы сможете разблокировать устройство с помощью PIN-кода устройства, графического ключа или отпечатка пальца.

Чтобы защитить приложение Kaspersky от несанкционированного удаления:

1. На нижней панели вкладок приложения «Лаборатория Касперского» нажмите **Все функции**.
2. Нажмите **Где мое устройство**.
3. Разблокируйте доступ к функции с помощью секретного кода, графического ключа или отпечатка пальца.
4. В разделе **Дополнительная защита** нажмите **Защита от удаления**.
5. Включите функцию.

Приложение Kaspersky будет запрашивать секретный код, когда кто-то попытается удалить приложение с устройства. При попытке изменения системных параметров, влияющих на защиту устройства, будет происходить блокировка устройства.

Разблокировка устройства

Если вы заблокировали устройство через My Kaspersky, вы можете его разблокировать.

Чтобы разблокировать устройство, выполните следующие действия:

1. На экране заблокированного устройства нажмите  > **Разблокировать**.
2. Введите секретный код.
3. Нажмите **ОК**.

Ваше устройство будет разблокировано.

Если вы не помните секретный код, вы можете восстановить его на My Kaspersky.

Использование блокировки экрана

О настройках блокировки экрана

Блокировка экрана позволяет предотвратить несанкционированный доступ к функциям, приложениям или настройкам.

Вы можете заблокировать экран с помощью следующих типов блокировки:

- секретный код;
- графический ключ;
- отпечаток пальца.

На устройствах Huawei также можно установить блокировку экрана с помощью распознавания лица.

Все типы блокировки экрана защищают доступ к следующим функциям и настройкам:

- настройки функций "Где мое устройство" и "Блокировка приложений"
- приложения, заблокированные вами, с помощью функции "Блокировка приложений";
- удаление приложения Kaspersky;
- настройки блокировки экрана.

Только секретный код может быть использован для следующих действий:

- изменение или восстановление секретного кода;
- разблокировка устройства, заблокированного на My Kaspersky.

Добавление секретного кода

Приложение предлагает установить секретный код приложения при первоначальной настройке функции "Где мое устройство" или Блокировки приложений. Вы сможете изменить секретный код в любое время.

Секретный код приложения должен состоять из 4 или более цифр.

На устройствах некоторых производителей после блокировки устройства секретный код становится системным PIN-кодом. Производители могут ограничивать количество символов, допустимых в системном PIN-коде. Чтобы избежать возможных проблем с разблокировкой устройства, мы рекомендуем установить секретный код с тем же количеством символов, что и в системном PIN-коде.

Если вы забыли секретный код, вы можете восстановить его на My Kaspersky или на устройстве.

Изменение секретного кода

Чтобы изменить секретный код, выполните следующие действия:

1. На нижней панели вкладок приложения Kaspersky нажмите **Профиль** > **Настройки** > **Блокировка экрана** > **Изменить секретный код**.
2. Введите текущий секретный код приложения.
3. Введите новый секретный код.
4. Подтвердите новый секретный код.

Новый секретный код установлен.

Восстановление секретного кода

Если вы забыли секретный код, вы можете восстановить его на устройстве или на сайте My Kaspersky.

Если на устройстве нет доступа в интернет, вы можете восстановить секретный код только на сайте My Kaspersky.

Чтобы восстановить секретный код на устройстве, выполните следующие действия:

Эта опция восстановления секретного кода доступна только в том случае, если устройство не защищено системной блокировкой устройства.

1. В окне с запросом секретного кода нажмите **Я не помню код**.
2. Введите пароль от вашего аккаунта My Kaspersky.
3. Нажмите **Сбросить секретный код**.
4. Введите новый секретный код.
5. Подтвердите новый секретный код.

Новый секретный код установлен.

Чтобы восстановить секретный код на сайте My Kaspersky, выполните следующие действия:

1. Откройте My Kaspersky на любом устройстве.
2. Войдите на My Kaspersky с аккаунтом, который использовался для настройки функции.
3. Перейдите в раздел **Устройства**.
   Откройте панель мобильного устройства, которым вы хотите управлять дистанционно.
4. На закладке **Код восстановления** нажмите на кнопку **Получить код**.
   На сайте отобразится код восстановления.
5. Введите код восстановления в приложении Kaspersky на устройстве.
6. Нажмите **Сбросить секретный код**.
7. Введите новый секретный код.
8. Подтвердите новый секретный код.

Новый секретный код установлен.

Добавление графического ключа

Если вы уже установили секретный код, вы можете добавить графический ключ. В приложении Kaspersky и в системных настройках вашего устройства используются разные графические ключи.

Чтобы защитить доступ к функциям приложения Kaspersky,

1. Задайте секретный код.
2. В окне **Секретный код** установлен нажмите **Установить графический ключ**.

   Вы можете добавить или поменять графический ключ позже в разделе **Настройки** > **Блокировка экрана**.

3. Следуйте инструкциям мастера установки графического ключа.

   Ваш графический ключ может включать в себя от 4 до 9 точек, соединенных между собой.

Если вы забыли свой графический ключ, выполните следующие действия:

1. Используйте секретный код.
2. Перейдите в **Настройки** > **Блокировка экрана**.
3. Нажмите **Установить графический ключ** и задайте новый ключ.

Об отпечатке пальца

Если вы уже установили секретный код, вы можете также добавить защиту от несанкционированного доступа с помощью отпечатка пальца. Приложение Kaspersky использует те же отпечатки пальцев, что и в настройках вашего устройства. Если вы еще не добавили отпечаток пальца, вы будете перенаправлены в настройки вашего устройства.

Чтобы использовать отпечатки пальцев для защиты доступа к настройкам и функциям приложения Kaspersky, установите флажок **Доступ по отпечатку пальца** в мастере первоначальной настройки или нажмите **Настройки** > **Блокировка экрана**.

Фильтр звонков

О Фильтре звонков

Фильтр звонков позволяет блокировать нежелательные звонки, например, звонки рекламного характера. Приложение фильтрует звонки по списку запрещенных номеров, который вы создаете. Для запрещенных контактов ваш номер будет занят.

"Лаборатория Касперского" постоянно улучшает защиту от спама в своих продуктах. Если вы используете Фильтр звонков в России, Индонезии и в Республике Казахстан, вы можете помочь приложению Kaspersky в обнаружении спамеров. Для этого вам нужно дать согласие на отправку статистики ваших звонков при первом запуске Фильтра звонков или позднее в разделе **О приложении** > **Положение об обработке данных для функциональности "Фильтр звонков"**.

Чтобы начать использовать Фильтр звонков, добавьте нежелательные контакты и номера в список запрещенных. Затем включите фильтрацию и при необходимости настройте подсказку после звонка.

«Фильтр звонков» не работает на планшетах, не имеющих слота для SIM-карты или функции мобильного телефона.

Управление списком запрещенных номеров

Запрещенные номера — это список номеров, с которых вы не хотите получать телефонные звонки. Чтобы заблокировать звонок с номера, добавьте этот номер в список. Контакты, добавленные в список запрещенных, больше не смогут до вас дозвониться. Вы можете добавить номера в запрещенные из контактов вашего телефона или вручную.

Когда вы добавляете номер в список запрещенных на устройствах с Android 9-13, этот номер автоматически добавляется в список контактов на вашем устройстве.

Если вы хотите разблокировать контакт, удалите его из списка запрещенных номеров. Вы снова можете принимать звонки от этого контакта.

Если на вашем телефоне установлено две SIM-карты, Фильтр звонков не блокирует входящие звонки на второй линии.

Как добавить номер в список запрещенных?

1. На нижней панели вкладок приложения «Лаборатория Касперского» нажмите **Все функции**.
2. Нажмите **Фильтр звонков**.

3. В блоке **Запрещенные номера** нажмите **Добавить**.
4. Укажите информацию для запрещенного контакта.
5. Нажмите **Добавить**, чтобы сохранить добавленный контакт.

   Контакт будет добавлен в список запрещенных номеров, и количество нежелательных контактов увеличится на один.

   Все звонки с этого номера будут заблокированы.

Как добавить номер в список запрещенных сразу после звонка?

Если вам позвонили с телефонного номера не из списка ваших контактов и функция **Подсказка после звонка** включена, приложение предложит вам заблокировать этот номер после звонка.

В окне подсказки выберите одно из следующих действий:

- **Блокировать звонки**, если вы хотите заблокировать звонки с этого номера.
- **Пропустить**, если вы хотите получать звонки с этого номера.

Если вы выберите заблокировать этот номер, он будет добавлен в список запрещенных номеров, и количество нежелательных контактов увеличится на один.

Все звонки с этого номера будут заблокированы.

Как отредактировать контакт в списке запрещенных номеров?

1. На нижней панели вкладок приложения «Лаборатория Касперского» нажмите **Все функции**.
2. Нажмите **Фильтр звонков**.
3. В блоке **Запрещенные номера** выберите контакт, который вы хотите изменить.
4. Измените данные контакта.
5. Сохраните измененный контакт.

   Информация о контакте в списке запрещенных номеров будет обновлена, и звонки от этого контакта будут заблокированы.

Как удалить контакт из списка запрещенных номеров?

1. На нижней панели вкладок приложения «Лаборатория Касперского» нажмите **Все функции**.
2. Нажмите **Фильтр звонков**.
3. В блоке **Запрещенные номера** выполните одно из следующих действий:
   - Выберите контакт, который вы хотите удалить из списка, и нажмите **Удалить контакт**.
4. Подтвердите удаление.

   Контакт будет удален из списка запрещенных номеров, и количество нежелательных контактов уменьшится на один.

   Теперь вы будете получать звонки с этого номера.

Настройка фильтрации

Чтобы включить фильтрацию звонков:

1. В нижнем меню приложения Kaspersky нажмите **Все функции**.
2. Нажмите **Фильтр звонков**.
3. Включите переключатель **Блокировать звонки от запрещенных номеров**.

   Звонки от контактов из вашего списка запрещенных номеров теперь будут блокироваться.

Вы также можете включить или выключить подсказку, предлагающую блокировать незнакомый номер. Эта подсказка отображается сразу после звонка с номеров, не найденных в вашем списке контактов. С помощью этой подсказки вы можете быстро добавить неизвестный номер в список запрещенных. Подробную информацию вы можете найти в разделе Как добавить номер в список запрещенных сразу после звонка.

Опция **Уведомлять после звонка** доступна только пользователям в России, Индонезии и в Республике Казахстан.

Чтобы включить подсказку:

1. В нижнем меню приложения Kaspersky нажмите **Все функции**.
2. Нажмите **Фильтр звонков**.
3. Включите переключатель **Уведомлять после звонка**.

Теперь после завершения или отклонения звонка вы будете видеть подсказку.

Если на вашем устройстве установлено приложение Kaspersky Who Calls, приложение Kaspersky будет использовать настройки подсказки из этого приложения. В этом случае вы можете изменять настройки подсказки в Kaspersky Who Calls. Обратите внимание, что приложение Kaspersky Who Calls доступно только в России, Индонезии и в Республике Казахстан.

Мои приложения и разрешения

О функции "Мои приложения"

Компонент Мои приложения позволяет оптимизировать пространство устройства и контролировать возможные риски для вашего устройства.

В разделе **Разрешения** экрана Мои приложения вы можете управлять разрешениями, которые вы выдали установленным на устройстве приложениям.

В разделе **Приложения** экрана "Мои приложения" вы можете просмотреть список приложений, установленных на устройстве (кроме системных приложений и приложения Kaspersky), узнать, какими приложениями вы не пользуетесь, удалить их и освободить место на вашем устройстве.

Анализ приложений

Первоначальная настройка компонента Мои приложения

1. На нижней панели вкладок приложения «Лаборатория Касперского» нажмите **Все функции**.
2. Прокрутите вниз до раздела **Производительность** и нажмите **Мои приложения**.
3. Перейдите в раздел **Приложения**.
4. Разрешите приложению Kaspersky доступ к истории использования приложений:

a. Ознакомьтесь с инструкциями и нажмите **Продолжить**.

Откроется список приложений, которые могут иметь доступ к истории использования приложений.

b. Выберите в списке приложение Kaspersky.

c. Включите переключатель **Доступ к истории использования**.

d. Вернитесь в приложение Kaspersky.

Компонент Мои приложения готов к использованию. Откроется список приложений, установленных на устройстве.

Просмотр установленных приложений

1. В разделе **Все функции** приложения Kaspersky нажмите **Мои приложения**.
2. Перейдите в раздел **Приложения**.

   Откроется список приложений, установленных на устройстве.
3. Чтобы отсортировать список, выберите критерии сортировки. Вы можете просматривать списки часто или редко используемых приложений. Внутри каждого списка можно отсортировать приложения по имени или по размеру.
4. Нажмите на имя приложения, чтобы узнать о нем больше.

Удаление неиспользуемого приложения

1. В разделе **Все функции** приложения Kaspersky нажмите **Мои приложения**.
2. Перейдите в раздел **Приложения**.

   Если приложения редко используются на вашем устройстве, они отображаются в разделе **Редко используемые**. Вы можете оценить размер этих приложений и выбрать приложения, которые следует удалить в первую очередь.
3. Удалите приложение одним из следующих способов:

   - Нажмите рядом с именем приложения.
   - Нажмите на имя приложения, затем нажмите **Удалить**.

4. Подтвердите действие.

Выбранное приложение будет удалено. Поздравляем, вы освободили пространство на устройстве!

Удаление нескольких неиспользуемых приложений

1. В разделе **Все функции** приложения Kaspersky нажмите **Мои приложения**.
2. Перейдите в раздел **Приложения**.

   Если приложения редко используются на вашем устройстве, они отображаются в разделе **Редко используемые**. Вы можете оценить размер этих приложений и выбрать приложения, которые следует удалить в первую очередь.
3. Нажмите и удерживайте название любого приложения.

   Рядом с названием каждого приложения появятся флажки.
4. Установите флажки рядом с названиями приложений, которые требуется удалить.
5. Нажмите в правом верхнем углу экрана.
6. Подтвердите действие для каждого приложения.

Подтвержденные приложения будут удалены. Поздравляем, вы освободили пространство на устройстве!

Просмотр разрешений

Приложения могут запрашивать доступ к основным функциям устройства и собирать личные данные без вашего ведома. Несмотря на то что некоторые разрешения необходимы приложениям для полноценного функционирования, многие предоставляемые разрешения являются потенциально небезопасными. Теперь вы можете просматривать и контролировать все разрешения, которые вы предоставили установленным приложениям.

Необходимо решить, хотите ли вы разрешать приложению выполнение определенных действий на вашем устройстве или использование определенных функций (например, камеры или микрофона).

Вы можете просматривать информацию об опасных и особых разрешениях. Опасные разрешения могут нанести ущерб личным данным пользователя и хранимой на устройстве информации (например, получив доступ к контактам, камере, местоположению, SMS). Особые разрешения требуют авторизации пользователя для изменения системных настроек.

Чтобы просмотреть список приложений, имеющих определенное разрешение,

нажмите на название разрешения.

Чтобы просмотреть, какие разрешения есть у приложения,

нажмите на название приложения и прокрутите экран вниз до раздела **Разрешения**.

Поиск утечки данных

О функции "Поиск утечки данных"

Функция "Поиск утечки данных" ищет ваши личные данные как в интернете, так и в даркнете (от номеров ваших кредитных карт до информации социального страхования). Если ваши данные станут общедоступными, функция "Поиск утечки данных" оповестит вас.

Если у вас нет подписки Kaspersky Plus или Premium, вам доступна ограниченная функциональность компонента: приложение проверяет на утечку только сервисы, привязанные к вашей почте, указанной для аккаунта My Kaspersky. Кроме того, проверку необходимо запускать вручную. Полная функциональность и автоматическая проверка аккаунтов на утечки данных доступна в тарифном плане Kaspersky Plus или Premium.

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

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 приложение Kaspersky, вы можете проверить на предмет возможной утечки данных не только свои, но и другие учетные записи, например, учетные записи ваших близких и друзей.

С тарифным планом Kaspersky Plus или Premium вы можете настроить автоматическую проверку еще 50 аккаунтов в добавок к вашему аккаунту My Kaspersky.

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

Проверка аккаунта на утечки

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

1. Откройте приложение Kaspersky.
2. Нажмите на раздел **Проверка утечки данных** на главном экране приложения.
3. Войдите в аккаунт My Kaspersky, если приложение предложит это сделать.

   После этого проверка аккаунта на утечки начнется автоматически.
4. Если вы ранее уже вошли в свой аккаунт My Kaspersky, нажмите на **Найти утечки**.

   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. Кроме того, приложение посоветует, что делать, если ваши данные утекли.

   Чтобы узнать подробную информацию о возможной утечке данных и рекомендациях "Лаборатории Касперского", нажмите на веб-сайт.
5. Приложение сохраняет все проверенные аккаунты в специальный список и проверяет аккаунты из этого списка каждый день.

При обнаружении возможной утечки данных вы получите уведомление.

Если ранее вы использовали на своем устройстве компонент "Проверка учетных записей" в приложении Kaspersky Security Cloud, ваш список электронных адресов будет скопирован в компонент "Поиск утечки данных" в приложении Kaspersky на том же устройстве. Для этого в обоих приложениях должна быть активирована подписка Personal или Family или Kaspersky Plus или Premium.

Безопасное VPN-соединение

«Лаборатория Касперского» приостанавливает работу и продажи Kaspersky Secure Connection на территории Российской Федерации. Работа бесплатной версии Kaspersky Secure Connection приостановлена с 15 ноября 2022 года./nПриобрести подписку на Kaspersky Secure Connection на официальном сайте «Лаборатории Касперского» и в магазинах мобильных приложений вы можете до прекращения продаж.
Продажи подписок будут приостановлены в 2023 году только на территории Российской Федерации. В связи с этим «Лаборатория Касперского» не может гарантировать возможность стабильного VPN-соединения до окончания срока действия подписки.»

О безопасном VPN-соединении

Безопасное VPN-соединение 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

Безопасное VPN-соединение 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 бесплатную версию Безопасного VPN-соединения. Вы можете перейти на безлимитную версию.

Теперь вы можете пользоваться безопасным VPN-соединением в нашем расширенном приложении Kaspersky для Android, объединившем в себе сразу несколько других. В этом приложении есть всё, что необходимо для защиты и приватности, а также все функции из Kaspersky Security Cloud и Kaspersky Secure Connection.

После установки приложения Kaspersky перейдите в раздел "Безопасное VPN-соединение" и следуйте инструкции на экране, чтобы перенести ваши настройки безопасного VPN-соединения.

После переноса настроек, безопасное VPN-соединение будет доступно только в приложении Kaspersky. Эта функция не будет доступна в Kaspersky Security Cloud и Kaspersky Secure Connection, и вы сможете удалить эти приложения.

Безопасное VPN-соединение будет автоматически выключено на время переноса настроек безопасного соединения в приложении Kaspersky.

Если вы хотите перенести настройки безопасного VPN-соединения, оба приложения должны быть подключены к одному аккаунту My Kaspersky. Если у вас есть разные подписки и вы хотите использовать их одновременно, обратитесь в Службу технической поддержки.

Вы все еще можете передумать и использовать Kaspersky Secure Connection вместо приложения Kaspersky. Однако настройки нельзя перенести обратно из приложения Kaspersky. Если вы решите продолжить использовать Kaspersky Security Cloud или Kaspersky Secure Connection, вам придется настраивать безопасное VPN-соединение вручную.

О подписке

Если у вас есть аккаунт My Kaspersky с подпиской на Kaspersky Secure Connection, вы можете использовать этот аккаунт для входа в приложение Kaspersky и пользоваться подпиской там.

Если вы использовали анонимную подписку для Kaspersky Secure Connection, вам нужно будет войти в ваш аккаунт My Kaspersky. В результате ваша подписка перестанет быть анонимной.

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

Недоступность VPN в отдельных регионах

В отдельных регионах использование VPN регулируется на законодательном уровне. Чтобы узнать больше, обратитесь к этой статье.

Перенос настроек безопасного VPN-соединения в приложение Kaspersky

Теперь вы можете пользоваться безопасным VPN-соединением в нашем расширенном приложении Kaspersky для Android, объединившем в себе сразу несколько других. В этом приложении есть всё, что необходимо для защиты и приватности, а также все функции из Kaspersky Security Cloud и Kaspersky Secure Connection.

После установки приложения Kaspersky перейдите в раздел "Безопасное VPN-соединение" и следуйте инструкции на экране, чтобы перенести ваши настройки безопасного VPN-соединения.

После переноса настроек, безопасное VPN-соединение будет доступно только в приложении Kaspersky. Эта функция не будет доступна в Kaspersky Security Cloud и Kaspersky Secure Connection, и вы сможете удалить эти приложения.

Безопасное VPN-соединение будет автоматически выключено на время переноса настроек безопасного соединения в приложении Kaspersky.

Если вы хотите перенести настройки безопасного VPN-соединения, оба приложения должны быть подключены к одному аккаунту My Kaspersky. Если у вас есть разные подписки и вы хотите использовать их одновременно, обратитесь в Службу технической поддержки.

Вы все еще можете передумать и использовать Kaspersky Secure Connection вместо приложения Kaspersky. Однако настройки нельзя перенести обратно из приложения Kaspersky. Если вы решите продолжить использовать Kaspersky Security Cloud или Kaspersky Secure Connection, вам придется настраивать безопасное VPN-соединение вручную.

О подписке

Если у вас есть аккаунт My Kaspersky с подпиской на Kaspersky Secure Connection, вы можете использовать этот аккаунт для входа в приложение Kaspersky и пользоваться подпиской там.

Если вы использовали анонимную подписку для Kaspersky Secure Connection, вам нужно будет войти в ваш аккаунт My Kaspersky. В результате ваша подписка перестанет быть анонимной.

Бесплатная версия Kaspersky Secure Connection

Вы можете использовать бесплатную или безлимитную версию безопасного VPN-соединения.

При использовании бесплатной версии:

- Вам доступен ограниченный объем защищенного трафика в день.
- Вы не можете выбирать виртуальный сервер. Виртуальный сервер выбирается автоматически.

При достижении лимита защищенного трафика безопасное VPN-соединение прерывается. 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.

> 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 безопасного VPN-соединения.

Вы можете получить неограниченный объем защищенного трафика, перейдя на безлимитную версию Kaspersky Secure Connection.

Безлимитная версия Kaspersky Secure Connection

При использовании *ограниченной версии*:

- Вам доступен ограниченный объем защищенного трафика в день.
- Вы не можете выбирать виртуальный сервер. Виртуальный сервер выбирается автоматически.

При использовании *безлимитной версии*:

- Вам доступен неограниченный объем защищенного трафика в день на пяти устройствах, подключенных к одному аккаунту My Kaspersky, вне зависимости от платформы устройства (Android или iOS). Если вы приобрели подписку в приложении, вы можете использовать ее и на других своих устройствах. На сайте My Kaspersky можно выбрать устройства, на которых вы хотите использовать безлимитную версию. Более подробная информация приведена в справке My Kaspersky .

- Вы можете выбрать виртуальный сервер и определяться в интернете как пользователь из любой страны, которая есть в списке.

Для перехода на безлимитную версию вам нужно оформить подписку на безопасное VPN-соединение. Вы можете оформить или продлить подписку в приложении.

> Для перехода на безлимитную версию и ее использования необходимо подключение к My Kaspersky.

В сведениях об аккаунте My Kaspersky указано количество дней, оставшихся до окончания срока действия подписки. Более подробная информация приведена в разделе "Просмотр информации о подписке".

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 бесплатной 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 безопасного VPN-соединения.

Чтобы посмотреть состояние безопасного VPN-соединения и доступный объем защищенного трафика, выполните одно из следующих действий:

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

Объем использованного и доступного защищенного трафика отобразится в нижней части экрана.

- Откройте панель уведомлений на устройстве.

  Объем использованного и доступного защищенного трафика отобразится в уведомлении.

Активация безлимитной версии безопасного VPN-соединения

Для перехода на безлимитную версию безопасного VPN-соединения можно воспользоваться аккаунтом My Kaspersky. В этом случае подписка на безлимитную версию будет связана с вашим аккаунтом My Kaspersky.

Если у вас нет аккаунта My Kaspersky, не обязательно незамедлительно создавать его. Переход на безлимитную версию безопасного VPN-соединения можно выполнить непосредственно из приложения, без аккаунта My Kaspersky. Затем, при необходимости, можно связать подписку на безлимитную версию с аккаунтом My Kaspersky.

Чтобы перейти на безлимитную версию, выполните следующие действия:

1. Перейдите в раздел безопасного VPN-соединения.
2. В нижней части экрана нажмите **Получить больше**.

   Пролистайте экраны с описанием функций и выберите безлимитную версию.
3. Выберите подписку на месяц или на год.

   В приложении откроется окно магазина Google Play.
4. Подтвердите покупку.

   Информация о подписке обновится на сайте My Kaspersky и на всех ваших устройствах, использующих безопасное VPN-соединение.

   Вы можете просмотреть детали подписки в разделе информации об аккаунте в приложении.

При приобретении автоматически продлеваемой подписки на Google Play, предлагается короткий ознакомительный период, во время которого можно пользоваться премиум-версией безопасного VPN-соединения бесплатно. Этот период предоставляется только один раз.

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

По истечении бесплатного периода приложение продолжает использовать безлимитную подписку с автоматическим продлением каждый расчетный период. Стоимость подписки будет автоматически списываться с вашего счета в Google Play.

Восстановление безлимитной версии безопасного VPN-соединения

Если ранее вы приобретали подписку на безлимитную версию безопасного VPN-соединения, вы можете восстановить ее. Подписка связана с вашим аккаунтом My Kaspersky.

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

Настройка Smart Protection

Об Умной Защите в безопасном VPN-соединении

Технология **Умной защиты** предлагает включить безопасное VPN-соединение, когда вы подключаетесь к интернету через незащищенную сеть Wi-Fi или открываете сайты и приложения, где нужно вводить конфиденциальную информацию.

Например, когда вы открываете сайт из категории **Банки**, приложение предлагает включить безопасное VPN-соединение, чтобы вы могли безопасно выполнять финансовые операции.

Вы можете настроить правила автоматического включения безопасного VPN-соединения для сетей, сайтов или приложений, которые вы часто используете.

Для использования этой функции необходимо включить специальные возможности для приложения Kaspersky.

Как включить специальные возможности

1. Перейдите в системные настройки устройства и нажмите **Специальные возможности**.
2. В списке приложений найдите приложение Kaspersky и нажмите на него.
3. Включите переключатель для приложения Kaspersky.

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.

Разрешите приложению Kaspersky 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.

На устройствах с Android 9-13 приложение запрашивает разрешение на доступ к геолокации вашего устройства, чтобы получать информацию о Wi-Fi сети (идентификаторы SSID, BSSID). Приложение использует эти данные для проверки сетей Wi-Fi и включения VPN, а также для определения домашней сети Wi-Fi и уведомления о подключенных устройствах. Приложение не использует доступ к геолокации для определения местоположения устройства.

Без доступа к вашей геолокации функция "Мониторинг умного дома" будет работать неправильно.

Приложение Kaspersky не имеет доступа к данным GPS и не отслеживает ваше фактическое местонахождение. Разрешение требуется только для получения информации о сети Wi-Fi (SSID, BSSID).

Чтобы предоставить приложению доступ к геолокации, убедитесь, что использование геолокации включено на вашем устройстве, а затем предоставьте доступ к геолокации специально для приложения Kaspersky. На некоторых устройствах разрешения требуется предоставлять вручную.

Безопасное VPN-соединение для приложения

Для использования этой функции необходимо включить специальные возможности для приложения Kaspersky.

Чтобы настроить автоматическое включение безопасного VPN-соединения для приложения, выполните следующие действия:

1. Перейдите в раздел безопасного VPN-соединения.

2. Нажмите **Настройки** > **Умная защита**.

3. Нажмите **Приложения**.

4. Выберите приложение из списка приложений на устройстве.

5. Выберите **При запуске приложения** и укажите, какое действие должно выполняться при открытии выбранного приложения:

   - **Включать безопасное VPN-соединение**. При открытии этого приложения приложение Kaspersky будет включать безопасное VPN-соединение.

   - **Спрашивать**. При открытии этого приложения отобразится уведомление с предложением включить безопасное VPN-соединение.

     Разрешите приложению Kaspersky 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.

   - **Не реагировать**. При открытии этого приложения приложение Kaspersky не будет включать безопасное VPN-соединение.

6. Нажмите **Применить**.

7. Нажмите **Виртуальный сервер** и выберите виртуальный сервер, который вы хотите использовать при открытии приложения.

Безопасное VPN-соединение для сайта

Рекомендуется защищать соединение при открытии сайтов, на которых вы вводите персональные данные. В противном случае ваши данные могут быть доступны злоумышленникам.

Для использования этой функции необходимо включить специальные возможности для приложения Kaspersky.

Чтобы настроить автоматическое включение безопасного VPN-соединения для определенного сайта, выполните следующие действия:

1. Перейдите в раздел безопасного VPN-соединения.

2. Нажмите **Настройки** > **Умная защита**.
3. Нажмите **Сайты**.
4. Убедитесь, что переключатель включен.
5. Нажмите **Другие сайты**.
6. Чтобы добавить сайт, нажмите  .

   Откроется окно **Добавить сайт**.
7. В поле веб-адреса введите адрес сайта и нажмите **ОК**.
8. Нажмите **При открытии сайта** и укажите, какое действие должно выполнять приложение при открытии этого сайта:

   - **Включать безопасное VPN-соединение**. При открытии этого сайта включается безопасное VPN-соединение. Например, вы можете настроить автоматическое включение безопасного VPN-соединения при открытии сайта вашего банка.
   - **Спрашивать**. При открытии этого сайта отображается уведомление с предложением включить безопасное VPN-соединение.

     > Разрешите приложению Kaspersky 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.

   - **Не реагировать**. При открытии этого сайта безопасное VPN-соединение не включается.
9. Нажмите **Применить**.
10. Нажмите **Виртуальный сервер** и выберите виртуальный сервер, который вы хотите использовать при открытии сайта.
11. Нажмите **Сохранить**.

Безопасное VPN-соединение для категории сайтов

Рекомендуется защищать соединение при открытии сайтов, на которых вы вводите персональные данные. В противном случае ваши данные могут быть доступны злоумышленникам. Например, вы можете настроить автоматическую защиту соединения при открытии сайтов платежных систем или социальных сетей.

Для использования этой функции необходимо включить специальные возможности для приложения Kaspersky.

Чтобы настроить автоматическое включение безопасного VPN-соединения для определенной категории сайтов, выполните следующие действия:

1. Перейдите в раздел безопасного VPN-соединения.
2. Нажмите **Настройки** > **Умная защита**.
3. Нажмите **Сайты**.
4. Убедитесь, что переключатель включен.
5. Выберите категорию сайтов:
   - **Банки**.
   - **Платежные системы**.
   - **Интернет-магазины**.
   - **Социальные сети**.
6. Укажите действие, которое должно выполняться при открытии сайтов из указанной категории:
   - **Включать безопасное VPN-соединение**. При открытии сайтов из указанной категории включается безопасное VPN-соединение.
   - **Спрашивать**. При открытии сайтов из указанной категории отображается уведомление с предложением включить безопасное VPN-соединение.

     Разрешите приложению Kaspersky 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.

- **Не реагировать**. При открытии сайтов из указанной категории безопасное VPN-соединение не включается.

7. Нажмите **Применить**.

Настройка безопасного VPN-соединения для незащищенных сетей Wi-Fi

При подключении к сети Wi-Fi приложение Kaspersky 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. Перейдите в раздел безопасного VPN-соединения.
2. Нажмите **Настройки** > **Умная защита**.
3. Нажмите **При подключении к незащищенным сетям 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 приложению Kaspersky 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.

   - **Включать безопасное VPN-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.

4. Нажмите **Применить**.

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. Перейдите в раздел безопасного VPN-соединения.
2. Нажмите **Настройки** > **Умная защита**.
3. Нажмите **Для известных сетей 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.
   - **Включать безопасное VPN-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.
6. Нажмите **Применить**.

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.

Вы можете выбрать определенную страну для посещения интернет-магазинов или социальных сетей или настроить безопасное VPN-соединение для определенного сайта или приложения. Настройки безопасного VPN-соединения для сайтов имеют больший приоритет, чем настройки для категорий сайтов.

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

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

Смена виртуального сервера

Чтобы сменить виртуальный сервер:

1. Перейдите в раздел безопасного VPN-соединения.
2. Нажмите на название страны.
3. Выберите новое местоположение.

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

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

Настройка смены виртуального сервера

При переключении между приложениями, сайтами или категориями сайтов с разными настройками виртуального сервера, вы можете указать, какой сервер приложение Kaspersky должно использовать – текущий или указанный для открываемого приложения или сайта.

Вы можете настроить смену виртуального сервера, если используете безлимитную версию.

Чтобы настроить смену виртуального сервера, выполните следующие действия:

1. Перейдите в раздел безопасного VPN-соединения.
2. Нажмите **Настройки** > **Умная защита**.
3. Нажмите **Какой сервер использовать**.

4. Укажите, какое действие должно быть выполнено при переключении между приложениями, сайтами или категориями сайтов, для которых настроены разные виртуальные серверы:

   - **Выбранный в настройках**. Приложение меняет ваше виртуальное местоположение на то, которое указано для открываемого приложения или сайта.

   - **Текущий сервер**. Приложение не меняет ваше виртуальное местоположение. Вы продолжаете использовать текущий виртуальный сервер.

   - **Спрашивать**. Приложение показывает уведомление, в котором можно выбрать, менять ваше текущее виртуальное местоположение или нет.

     Если вы выберете не менять виртуальный сервер для указанного приложения или сайта, то приложение не будет предлагать изменить сервер для приложения или сайта в течение следующих 6 часов.

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, безопасному VPN-соединению 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 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. Перейдите в раздел безопасного VPN-соединения.
2. В разделе **Настройки** включите опцию **Блокировка трафика для защиты**.
3. 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.
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 безопасного VPN-соединения

Запрещается использование безопасного VPN-соединения 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 функции безопасного VPN-соединения.

Поиск небезопасных настроек

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 на устройстве не установлен пароль, то посторонние могут получить доступ к данным на вашем устройстве.

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.

Поиск небезопасных настроек выполняет поиск небезопасных настроек операционной системы не реже одного раза в день. При обнаружении небезопасных настроек операционной системы, вам предлагается их исправить, чтобы восстановить безопасность операционной системы.

Информация о найденных небезопасных настройках отображается в разделе **Поиск небезопасных настроек** в главном окне приложения. Нажмите на этот раздел, чтобы выполнить следующие действия:

- Просмотреть информацию о небезопасных настройках.

- Узнать, как исправить небезопасные настройки.

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

Исправление небезопасных настроек

Чтобы исправить небезопасные настройки операционной системы, выполните следующие действия:

1. Откройте главное окно приложения.
2. В разделе **Все функции** приложения Kaspersky нажмите **Поиск небезопасных настроек**, чтобы открыть экран функции.
3. Нажмите на небезопасную настройку, которую вы хотите исправить.

   Откроется описание небезопасной настройки и рекомендации по исправлению этой настройки.
4. Ознакомьтесь с предложенным решением и нажмите соответствующую кнопку.

   Откроется окно с системными настройками Android.
5. Измените настройку на рекомендованное значение.

Если вы хотите оставить небезопасную настройку без изменений и скрыть ее, нажмите  .

Вы можете просмотреть скрытые небезопасные настройки по кнопке  в правом верхнем углу экрана.

Безопасный QR-сканер

QR-код или штрих-код, сканируемый устройством, может содержать различную информацию. Эта информация может быть небезопасной для вашего устройства: например, содержать ссылку на фишинговый сайт. Безопасный QR-сканер позволяет сканировать QR-коды и штрихкоды и безопасно получать доступ к зашифрованной них информации. Перед тем, как открыть ссылку, функция проверяет ее на возможные угрозы и вирусы.

Вот инструкции по выполнению типичных пользовательских задач, которые предоставляет эта функция:

Сканирование QR-кода

Чтобы отсканировать код:

1. Наведите камеру на QR-код или штрих-код.
2. Держите устройство неподвижно в течение 1-2 секунд.

Безопасный QR-Сканер автоматически фокусирует изображение и расшифровывает информацию, зашифрованную в коде.

В зависимости от типа информации, зашифрованной в коде, на устройстве отображается текст, ссылка на веб-сайт, контактные данные или настройки подключения к сети Wi-Fi.

Безопасный QR-Сканер сохраняет все отсканированные коды в историю, если функция сохранения истории включена в настройках приложения.

Вы можете просмотреть актуальную информацию о результатах проверки содержимого QR-кода или штрих-кода в истории, нажав на нужную запись. Приложение снова проверяет ссылки и показывает актуальный результат.

Следуйте этим рекомендациям при сканировании кода:

- Если Безопасный QR-Сканер не может распознать код, переместите камеру поближе к коду или подальше от него, чтобы сфокусировать изображение.
- Если освещения недостаточно, нажмите на значок фонарика на экране функции, чтобы включить фонарик.

В разделе «Настройки» функции вы можете:

- Включить звуковое и виброподтверждение того, что код отсканирован;

  Виброподтверждение доступно только на устройствах, поддерживающих эту функцию.

- Включить историю, чтобы сохранять отсканированные коды;
- Выбрать, хотите ли вы получать запрос на открытие перед открытием ссылки из кода.

Открытие веб-сайта

Безопасный QR-Сканер сканирует веб-сайты на наличие онлайн-угроз перед их открытием. Для проверки приложение использует облачную службу Kaspersky Security Network. Безопасный QR-Сканер предупреждает о ссылках на веб-сайты, известные облачному сервису Kaspersky Security Network как представляющие угрозу для пользователей. Приложение выделяет такие ссылки красным цветом и не позволяет открывать их в браузере или сохранять в контактах вашего устройства.

Чтобы открыть веб-сайт:

1. Наведите камеру на код с зашифрованной ссылкой на сайт.

   Безопасный QR-Сканер автоматически фокусирует изображение и расшифровывает ссылку, зашифрованную в коде, затем проверяет ссылку на наличие угроз. Если ссылка безопасна, приложение предложит вам открыть ее в браузере вашего устройства по умолчанию.

2. Если вы не хотите получать запрос об открытии безопасных ссылок, вы можете отключить этот запрос в настройках функции.

Добавление контакта

Безопасный QR-сканер может распознавать контактные данные, закодированные в QR-коде.

После расшифровки QR-кода вы сможете:

- Посмотреть содержимое карточки контакта;
- Позвонить контакту, если в карточке контакта указан номер мобильного телефона;
- Отправить SMS-сообщение контакту, если в карточке контакта указан номер мобильного телефона;
- Создать этот контакт в списке контактов вашего устройства.

Если в каком-либо поле контактных данных были обнаружены вредоносные или фишинговые ссылки, добавить эти ссылки в карточку контакта на вашем устройстве невозможно.

Подключение к сети Wi-Fi

Чтобы подключиться к сети Wi-Fi:

1. Наведите камеру на QR-код с зашифрованными настройками подключения к сети Wi-Fi.

   Безопасный QR-сканер автоматически фокусирует изображение и расшифровывает QR-код. Откроется окно с настройками подключения к сети Wi-Fi:

- **SSID / Название сети**
- **Пароль**
- **Тип**

2. Нажмите **Сохранить сеть**. Если появится системный запрос, согласитесь сохранить сеть.
3. На следующем экране нажмите **Подключиться**.

Если вы используете устройство с Android 10 или ниже, для подключения к сети Wi-Fi:

1. Наведите камеру на QR-код с зашифрованными настройками подключения к сети Wi-Fi.

   Безопасный QR-сканер автоматически фокусирует изображение и расшифровывает QR-код. Откроется окно с настройками подключения к сети Wi-Fi:

   - **SSID / Название сети**
   - **Пароль**
   - **Тип**

2. Нажмите **Показать доступные сети**.

   Безопасный QR-Сканер скопирует пароль сети в буфер обмена. Появится окно со списком доступных сетей Wi-Fi.

3. Нажмите на название сети, которое появилось на шаге 1.
4. В открывшемся окне вставьте пароль из буфера обмена и нажмите **Подключить** .

Расход батареи

Работу этого компонента обеспечивает приложение Kaspersky Battery Life и компонент Battery Life в приложении Kaspersky.

Kaspersky Battery Life помогает экономнее расходовать заряд батареи, отслеживая запущенные приложения. Приложение Kaspersky Battery Life бесплатное. Вы можете установить его из Google Play. Kaspersky Battery Life не отображается в меню приложения после установки.

Kaspersky Battery Life отслеживает уровень заряда батареи устройства и уведомляет вас, если батарея скоро разрядится. После получения уведомления вы можете настроить параметры вашего устройства или закрыть отдельные приложения, чтобы продлить время работы вашего устройства без подзарядки.

Вы можете указать, за какое время до полной разрядки устройства приложение должно предупредить вас.

Kaspersky Battery Life может также отправлять статистику об уровне заряда батареи устройства в My Kaspersky. На My Kaspersky вы можете проверять уровень заряда батареи всех устройств, подключенных у вашему аккаунту My Kaspersky.

Просмотр отчетов приложения

Приложение Kaspersky постоянно формирует отчеты.

В отчетах вы можете просмотреть:

- информацию о работе Антивируса, например, результаты проверки, сведения о найденных угрозах, обновления;
- информацию о работе Интернет-защиты, например, заблокированные веб-сайты.

Отчеты сгруппированы по времени их создания. Вы можете настроить отображение отчетов для конкретного компонента приложения. Отчет может содержать до 50 записей. После того как число записей в отчете превысит 50, более ранние записи удаляются и замещаются новыми.

Чтобы посмотреть отчеты о работе приложения,

1. На главном экране приложения нажмите **Профиль**.
2. Выберите **Настройки**.
3. Нажмите **Отчеты**.

Использование My Kaspersky

О 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;

Вы можете зайти на My Kaspersky одним из следующих способов:

- использовать учетные данные других ресурсов "Лаборатории Касперского";
- Создать аккаунт My Kaspersky, если у вас ее еще нет (на сайте My Kaspersky или в совместимых с ним программах);
- -

Для работы с сайтом My Kaspersky вам нужно подключить к нему ваши устройства.

Подробная информация о работе с My Kaspersky доступна в справке My Kaspersky .

Об аккаунте My Kaspersky

Аккаунт My Kaspersky требуется для входа и работы с сайтом My Kaspersky , а также для работы с некоторыми программами "Лаборатории Касперского".

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

При создании уаккаунта My Kaspersky вам нужно указать действующий адрес электронной почты и придумать 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. Дополнительную информацию см. 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 будет отправлен уникальный код безопасности одним из следующих способов:

- по SMS Для этого используется номер телефона, указанный вами в My Kaspersky. Таким образом, для входа в аккаунт нужен и номер телефона, и пароль.
- через приложение проверки подлинности Сначала вам нужно настроить двухэтапную проверку по номеру вашего телефона, чтобы функция приложения проверки подлинности стала доступной.

Вы можете включить двухэтапную проверку на My Kaspersky. Если вы поменяли свой номер телефона, обновите его на My Kaspersky. Если вы вошли в аккаунт на устройстве до настройки двухэтапной проверки, ничего не изменится. Дополнительные инструкции см. в справке My Kaspersky.

У кода безопасности короткий срок действия. После его истечения вы можете запросить новый код.

Если вы не получили SMS-сообщение с кодом безопасности

1. Проверьте доступность мобильной сети.
2. Дождитесь появления кнопки **Запросить код повторно** в приложении.
3. Нажмите **Запросить код повторно**.

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

Управление приложением Kaspersky через My Kaspersky

На сайте My Kaspersky можно просмотреть состояние защиты вашего устройства и удаленно управлять некоторыми функциями приложения Kaspersky, например:

- обновить антивирусные базы приложения;
- включить Автоматический Антивирус, если он был выключен;
- приобрести или обновить подписку на использование приложения Kaspersky;
- управлять функциями "Где мое устройство": защитить данные на устройстве в случае кражи или потери (например, вы можете удаленно заблокировать устройство или узнать

его местоположение);

- восстановить секретный код.

Обновление баз приложения

Вы можете обновить базы приложения на сайте My Kaspersky.

Чтобы запустить обновление через My Kaspersky :

1. Откройте My Kaspersky на любом устройстве.
2. Войдите на My Kaspersky с аккаунтом, который использовался для настройки функции.
3. Перейдите в раздел **Устройства**.

   Откройте панель мобильного устройства, которым вы хотите управлять дистанционно.
4. На закладке **Состояние защиты** в блоке **Антивирус** нажмите на кнопку **Обновить**.

Обновление баз будет запущено на устройстве.

Поделиться учетными данными My Kaspersky по ссылке

Если вы приобрели подписку на приложение Kaspersky для нескольких устройств, вы можете создать персональную ссылку для установки приложения Kaspersky 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 приложение Kaspersky на другое устройство, выполните следующие действия:

1. В разделе **Профиль** приложения Kaspersky нажмите **Поделиться подпиской**.
2. В появившемся окне нажмите **Отправить ссылку**.

   Отобразится системное окно с вариантами, как можно поделиться ссылкой.
3. Откройте ссылку на устройстве, на котором вы хотите установить приложение Kaspersky.

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

Настройка уведомлений приложения

По умолчанию в приложении Kaspersky для Android включен показ уведомлений о работе приложения: запуске, истечении срока действия подписки, включении или отключении защиты.

Чтобы включить или выключить уведомления:

1. На нижней панели вкладок приложения нажмите **Профиль**.
2. Выберите **Настройки**.
3. Установите или снимите флажок **Уведомления**.

Подборка новостей безопасности

Kaspersky показывает вам новости кибербезопасности, рекомендации по защите информации и варианты подписки на премиум-версию приложения. Когда приложение узнает, в какой защите вы особенно нуждаетесь, оно может предложить лучшие варианты этой защиты. Например: если вы часто подключаетесь к непроверенным сетям Wi-Fi (в кафе, торговых центрах и т.п.), приложение Kaspersky расскажет, как предотвратить утечку данных в таких случаях.

По умолчанию, эта информация будет регулярно показана вам внутри приложения. Если вы не хотите получать эту информацию, вы можете выключить функцию.

Чтобы выключить подборку новостей безопасности, выполните следующие действия:

1. В нижнем меню приложения нажмите **Профиль** > **Настройки**.
2. В разделе **Настройки приложения** снимите флажок **Сообщения** .

   Вы больше не будете получать подборку новостей безопасности от приложения.

Ранний доступ к функциям

В бесплатной версии приложения Kaspersky вы можете протестировать новые функции в приложении, чтобы мы смогли учесть ваш опыт в дальнейшем.

Мы можем включить новую функцию в приложении, для изучения вашего интереса и возможности получить отзыв о ней. Ранний доступ может быть предоставлен небольшой группе случайных пользователей. Поэтому не беспокойтесь, если ваше приложение не имеет функции, отмеченной в справке как Функция с ранним доступом. Обратите внимание, что функции с ранним доступом могут быть изменены или отключены.

Список функций с ранним доступом

Автоматическая проверка

Автоматическое обновление антивирусных баз: приложение само регулярно обновляет свои базы, так что вам не нужно обновлять их. Кроме того, на главном экране приложения нет кнопки **Обновление**.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или в других источниках информации о приложении, рекомендуется обратиться в Службу технической поддержки. Перейдите на сайт Службы технической поддержки , чтобы связаться с экспертами, которые помогут ответить на ваши вопросы по установке и использованию приложения.

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

Источники информации о приложении

Страница приложения Kaspersky на сайте "Лаборатории Касперского"

На этой странице вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница приложения Kaspersky содержит ссылку на интернет-магазин. В нем вы можете приобрести или продлить подписку.

Страница приложения Kaspersky в Базе знаний

База знаний — это раздел сайта Службы технической поддержки.

На этой странице вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к приложению Kaspersky, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ «Лаборатории Касперского» на форуме

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

На форуме можно просматривать опубликованные темы, добавлять комментарии и создавать новые темы для обсуждения.

Известные проблемы

Перейдите по ссылке ниже, чтобы ознакомиться с известными проблемами приложения:

Kaspersky для Android – Известные проблемы

Юридическая информация

Просмотр условий лицензионного соглашения и других юридических документов

Чтобы просмотреть юридический документ:

1. На нижней панели вкладок приложения нажмите **Профиль**.
2. Нажмите **О приложении** > **Юридическая информация**.

   Откроется окно **Правовая информация**.
3. Нажмите на название документа, который вы хотите просмотреть.

Отказ от согласия на передачу данных

Вы соглашаетесь на автоматическую отправку данных Правообладателю на регулярной основе исключительно по своему выбору. Если вы хотите отказаться от своего согласия отправлять данные, передаваемые в рамках Положения о Веб-портале, вы можете сделать это в любое время, отключив свое устройство от My Kaspersky.

[Как отключить устройство от вашего аккаунта My Kaspersky]

1. Зайдите в ваш аккаунт My Kaspersky.
2. Перейдите в раздел **Подписки** и выберите подписку, которую используете на устройстве, которое хотите отключить.
3. На следующем экране нажмите на название устройства.
4. Нажмите **Отключить устройство**. В появившемся окне нажмите **OK**.

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.

Android, Chrome, Firebase, Gmail, Google и Google Play – товарные знаки Google LLC.

Apple – товарный знак Apple Inc.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Intel, Atom – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

ARM – товарный знак или зарегистрированный товарный знак ARM Ltd. или дочерних компаний.

Huawei, HUAWEI HONOR, EMUI являются товарными знаками Huawei Technologies Co., Ltd.

SAMSUNG – товарный знак компании SAMSUNG в США или других странах.

ASUS Trademark, ZenFone являются зарегистрированными товарными знаками Asustek Computer Inc. в Соединенных Штатах Америки и/или в других странах.

HTC – товарный знак HTC Corporation.

-

Информация для бета-тестировщиков

О бета-версии

Бета-версия не предназначена для использования в Соединенных Штатах Америки. Бета-версии также недоступны для устройств Huawei.

Мы бы хотели узнать о вашем опыте использования новых функций наших мобильных продуктов и пригласить вас к участию в бета-тестировании. Бета-версия включает новые функции, которые вы можете испытать перед их официальным выпуском.

Обратите внимание, что бета-версии могут быть менее стабильны, чем последняя официально выпущенная публичная версия. Могут возникать проблемы, такие как аварийное завершение работы, неправильная работа функций или недоступность сервисов.

Бета-версия предоставляется бесплатно. Однако функциональность приложения может быть ограничена (например, могут быть недоступны покупки). Внимательно ознакомьтесь с условиями и положениями Лицензионного соглашения для бета-версии.

Вы должны использовать приложение только в рамках функциональности, которую предоставляет установленная версия приложения. Чтобы просмотреть список приложений, бета-версии которых вы используете, перейдите в Google Play и нажмите **Профиль** > **Мои приложения и игры** > **Бета-версии**.

Перед тем, как начать бета-тестирование приложения, внимательно прочтите раздел "Бета-версия и подписки".

Принять участие в бета-тестировании

Зарегистрироваться для участия в бета-тестировании можно одним из следующих способов:

- Перейдите на страницу бета-версии в Google Play и следуйте приведенным там инструкциям
- Отсканируйте следующий QR-код, и следуйте инструкциям.

Отправить отзыв

Вы можете оставить свои комментарии и замечания на странице бета-версии в Google Play.

Завершить бета-тестирование

Чтобы завершить бета-тестирование, перейдите на страницу бета-версии в Google Play и следуйте приведенным там инструкциям.

После завершения бета-тестирования вы сможете загрузить стандартную версию приложения из Google Play.

Бета-версия и подписки

Мы рекомендуем вам зарегистрировать отдельный аккаунт My Kaspersky, чтобы использовать его исключительно для бета-тестирования.

Если вы уже приобрели подписку, не добавляйте коды активации в аккаунт My Kaspersky, используемый для бета-тестирования. В противном случае приложение автоматически активирует подписку и срок действия вашей подписки начнет истекать. Узнайте, как проверить подписки на сайте My Kaspersky, в справке My Kaspersky .

Если вы уже используете приложение по подписке, вы можете протестировать бета-версию функций по той же подписке. При этом срок действия вашей подписки не будет продлен на время бета-тестирования.