kaspersky

Kaspersky Android

Руководство по эксплуатации

Версия программы: 11

Kaspersky
Standard | Plus | Premium

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	✓	✓	✓	✓
Устройства в моей сети	✗	✗	✓	✓
Другие приложения				
Kaspersky Battery Life	✓	✓	✓	✓
Kaspersky QR Scanner	✓	✓	✓	✓
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. Нажмите на  .

3. В верхней части меню нажмите на иконку  с информацией о подписке.

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. Нажмите **Купить подписку**.

6. 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. Нажмите на  .

3. Убедитесь, что вы вошли в ваш аккаунт My Kaspersky. В противном случае нажмите **Войти в My Kaspersky**.

4. В верхней части меню нажмите на иконку  с информацией о подписке.

5. 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.

   Если подписка, которую можно использовать для активации приложения, не найдена, нажмите **У меня есть подписка**.

6. Нажмите **Войти в My Kaspersky** и следуйте инструкциям на экране.

   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. Нажмите на  .
3. В верхней части меню нажмите на иконку  с информацией о подписке.
4. Нажмите **Купить или восстановить подписку**.
5. Выберите **У меня есть подписка**.
6. Нажмите **Ввести код активации**.
7. 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,

В панели быстрого запуска приложения Kaspersky нажмите **Обновление**.

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

Как запланировать автообновление

1. В главном окне приложения Kaspersky нажмите **Автоматический Антивирус**.
2. Выберите **Обновление**.
3. Нажмите **По расписанию** и выберите один из вариантов:
   - **Раз в неделю**: базы будут обновляться автоматически раз в неделю в указанные вами день и время.
   - **Раз в день**: базы будут обновляться автоматически один раз в день в указанное вами время.
   - **Выключено**: базы не будут обновляться автоматически. Вам нужно будет обновлять их вручную.
4. Чтобы указать день запуска обновления (доступно только для обновления раз в неделю), нажмите **День запуска** и выберите день.
5. Чтобы указать время запуска обновления (доступно для обновления раз в день и раз в неделю), нажмите **Время запуска** и установите время.

В данный момент мы работаем над улучшением этой функции. Изменения в ее работе – часть раннего доступа к функциям, поэтому они доступны только небольшой группе пользователей.

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 как часть Автоматического Антивируса.

  - 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.

О функции "Блокировка приложений"

Блокировка приложений позволяет защитить ваши данные от посторонних. Вы можете защитить доступ к приложениям, содержащим ваши личные данные, например, WhatsApp, Фото, Сообщения, Snapchat, Viber, Gmail, Настройки и многим другим. Если вы открываете приложение, защищаемое Блокировкой приложений, приложение Kaspersky попросит вас разблокировать доступ к этому приложению с помощью секретного кода, графического ключа или отпечатка пальца.

Приложение Kaspersky использует настройки устройства для защиты доступа к приложениям. Чтобы обеспечить защиту, мы рекомендуем:

- защитить доступ к приложению Настройки с помощью Блокировки приложений;
- включить защиту от несанкционированного удаления приложения Kaspersky, установив флажок **Защита от удаления** в настройках функции "Где мое устройство".

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 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. Нажмите на  .
3. В верхней части меню нажмите значок  с информацией о подписке или вашим адресом электронной почты, если вы вошли в My Kaspersky.
4. Откроется окно с информацией о подписке.
5. Нажмите **Подробнее**, чтобы просмотреть подробную информацию о вашей 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. Нажмите на  .
3. В верхней части меню нажмите на иконку  с информацией о подписке.
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. Нажмите **Купить подписку**.
6. 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. Нажмите на  .
3. Убедитесь, что вы вошли в ваш аккаунт My Kaspersky. В противном случае нажмите **Войти в My Kaspersky**.
4. В верхней части меню нажмите на иконку  с информацией о подписке.
5. 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.

   Если подписка, которую можно использовать для активации приложения, не найдена, нажмите **У меня есть подписка**.
6. Нажмите **Войти в My Kaspersky**и следуйте инструкциям на экране.

   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. Нажмите на  .
3. В верхней части меню нажмите на иконку  с информацией о подписке.
4. Нажмите **Купить или восстановить подписку**.
5. Выберите **У меня есть подписка**.
6. Нажмите **Ввести код активации**.
7. 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 подписок на приложение Kaspersky

Когда вы обновляете приложение Kaspersky Internet Security до приложения Kaspersky, ваша подписка также автоматически обновляется в соответствии с новыми планами подписки на приложение Kaspersky. Дополнительные сборы не взимаются. Все условия подписки, такие как срок действия или дата следующего автоматического продления, остаются прежними.

План подписки обновляется следующим образом:

- Если у вас была подписка на Kaspersky Internet Security для Android, вы перейдете на подписку Kaspersky Standard.
- Если у вас была подписка на Kaspersky Security Cloud Personal или Family, вы перейдете на подписку на Kaspersky Plus.
- Если у вас была подписка на Kaspersky VPN, у вас будет безлимитный VPN в приложении Kaspersky.

Чтобы продолжить использовать некоторые функции приложения по подписке, вам может потребоваться войти в свою учетную запись My Kaspersky.

Вход в My Kaspersky с помощью аккаунта Google

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

Вход в первый раз

Чтобы войти в My Kaspersky с помощью существующего аккаунта Google 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 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 5-12.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. Нажмите  > **О приложении** > **Правовая 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 отказаться от условий положения, нажмите **Выключить**.

Кроме того, вам будет предложено принять **Положение об обработке данных в целях предоставления функции VPN**, которое необходимо для работы функции безопасного VPN-соединения, и **Положение об обработке данных для обеспечения функциональности "Устройства в моей сети"**, которое необходимо для работы функции "Устройства в моей сети". 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 "Устройства в моей сети".

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

Отзыв согласия и выключение соответствующей функции

1. Нажмите  > **О приложении** >**Правовая информация**.
2. Нажмите на **Положение об обработке данных для обеспечения функциональности "Устройства в моей сети"** или на **Положение об обработке данных в целях предоставления функции VPN**.

   Откроется содержание выбранного положения.

3. Нажмите **Отклонить условия Положения**.
4. В появившемся окне нажмите **Выключить**.

Если вы не примете или отзовете принятие **Положение об обработке данных в целях предоставления функции VPN**, функция "Безопасное VPN-соединение" не будет работать. Если вы не примете или отзовете принятие **Положение об обработке данных для обеспечения функциональности "Устройства в моей сети"**, функция "Устройства в моей сети" 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 свои персональные данные, отправленные установленной версией приложения, из "Лаборатории Касперского", обратитесь в Службу технической поддержки и сообщите идентификаторы вашего устройства и установки.

Просмотр идентификаторов устройства и установки

Нажмите  > **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 11.84.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 11.85.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 главном окне приложения нажмите ☰ или смахните вправо.

   Слева появится панель быстрого доступа.

2. В боковом меню нажмите **О приложении** > Правовая 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.

В случае входа на Веб-Портал с помощью Вашей учетной записи в сервисе внешнего провайдера аутентификации Правообладателю необходимо получать и обрабатывать следующую информацию:

- идентификационный токен, полученный от провайдера аутентификации;
- тип данных, передаваемых провайдеру аутентификации;
- идентификатор Правообладателя в системе провайдера аутентификации;
- параметры, запрашиваемые у провайдера аутентификации;
- значение, генерируемое для верификации запроса.

Также могут обрабатываться следующие данные:

- URI, на который отправляется ответ провайдера аутентификации;
- признак установки приложения провайдера аутентификации на устройство;
- версия приложения провайдера аутентификации;
- имя провайдера аутентификации;
- идентификатор ресурса Правообладателя;
- тип токена;
- операционная система.

Обработка данных в сервисе провайдера аутентификации регулируется политиками провайдера.

Доступность сервисов провайдера аутентификации зависит от региона и версии используемого ПО и может отличаться по регионам и версиям.

Для обеспечения бесперебойной работы ПО поставщику Информационных систем третьих лиц необходимо получать и обрабатывать информацию о приобретённой лицензии, об установленном ПО и о Компьютере. Передаются следующие данные:

- идентификатор программного обеспечения;
- версия установленного ПО;
- признак работы ПО в фоновом режиме;
- архитектура ЦП;
- уникальный идентификатор события;
- дата и время события;
- модель устройства;
- объем полного и используемого дискового пространства;
- название и версия ОС;
- объём полной и используемой оперативной памяти;
- признак рутованности устройства;
- ориентация экрана в момент события;
- производитель продукта/устройства;
- уникальный идентификатор установки;
- версия отправляемой статистики;
- тип исключения ПО;
- текст сообщения об ошибке;
- признак того, что исключение ПО вызвано исключением на вложенном уровне;
- идентификатор потока;
- очередь, в которой был запущен поток;
- данные о сигнале, который привел к неожиданному завершению работы ПО: название сигнала, код сигнала, адрес сигнала;

- для каждого фрейма, ассоциированного с потоком, исключением или ошибкой: имя файла фрейма, номер строки файла фрейма, отладочные символы, адрес и смещение в бинарном образе, отображаемое имя библиотеки, содержащей фрейм, тип фрейма, признак того, что фрейм стал причиной ошибки;
- идентификатор ОС;
- признак того, что фрейм стал причиной ошибки ПО;
- признак того, что выполнение потока привело к неожиданному завершению работы ПО;
- идентификатор проблемы, связанной с событием;
- информация о событиях, предшествующих неожиданному завершению работы ПО: идентификатор события, дата и время события, тип события и значение;
- значения регистра ЦП.

Правообладатель не несёт ответственности за обработку данных, полученных поставщиком Информационных систем третьих лиц. Используя ПО, Вы должны ознакомиться с условиями и процедурами обработки данных, указанных в политике конфиденциальности поставщика Информационных систем третьих лиц.

Поставщик Информационных систем третьих лиц обрабатывает данные в соответствии с политикой конфиденциальности. Вы можете ознакомиться с ней по адресу https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms

О предоставлении данных (другие регионы)

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

- 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 11.85.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. Нажмите ☰ > **О приложении** > **Юридические документы**.
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 сервисах Google. Для предоставления этой функциональности Правообладателю и сторонним сервис-провайдерам необходимо получать и обрабатывать информацию в рамках настоящего Положения.

Правообладатель использует для обработки данных информационные системы третьих лиц. Обработка данных в информационных системах третьих лиц регулируется соответствующими политиками конфиденциальности таких систем. Правообладатель использует ниже указанные информационные системы третьих лиц для обработки перечисленных данных.

Данные обрабатываются в зависимости от выбираемого вами сервиса.

Google

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Google для их обработки для заявленных целей:

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

Передача данных в сервис Google осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Google доступна по адресу: https://policies.google.com/privacy.

В случае входа на Веб-Портал с помощью Вашей учетной записи в сервисе внешнего провайдера аутентификации Правообладателю необходимо получать и обрабатывать следующую информацию:

- идентификационный токен, полученный от провайдера аутентификации;
- тип данных, передаваемых провайдеру аутентификации;
- идентификатор Правообладателя в системе провайдера аутентификации;
- параметры, запрашиваемые у провайдера аутентификации;
- значение, генерируемое для верификации запроса.

Также могут обрабатываться следующие данные:

- URI, на который отправляется ответ провайдера аутентификации;
- признак установки приложения провайдера аутентификации на устройство;
- версия приложения провайдера аутентификации;
- имя провайдера аутентификации;

- идентификатор ресурса Правообладателя;
- тип токена;
- операционная система.

Обработка данных в сервисе провайдера аутентификации регулируется политиками провайдера.

Доступность сервисов провайдера аутентификации зависит от региона и версии используемого ПО и может отличаться по регионам и версиям.

Установка и удаление приложения

Аппаратные и программные требования

Эта справка применима для приложения Kaspersky версии 11.85.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 5.0–12.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.

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 .

Удаление приложения

Мы рекомендуем использовать меню приложения Kaspersky для удаления приложения.

Чтобы удалить приложение Kaspersky:

1. Откройте приложение Kaspersky.
2. Нажмите > **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,

В панели быстрого запуска приложения Kaspersky нажмите **Проверка** > **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,

В панели быстрого запуска приложения Kaspersky нажмите **Проверка** > **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 как часть Автоматического Антивируса.

  - 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. В панели быстрого запуска приложения Kaspersky нажмите **Проверка** > **Проверка папки**.
2. Выберите папку или файл для проверки.
3. Нажмите  для запуска проверки.

Настройка проверки по расписанию

Чтобы настроить проверку по расписанию:

1. В панели быстрого запуска приложения Kaspersky нажмите **Автоматический Антивирус** > **Ручная и регулярная проверки**.
2. Выберите действие приложения при обнаружении объекта во время проверки:
    a. Установите флажок **Лечить**, если требуется, чтобы приложение автоматически пыталось вылечить зараженный файл.
    b. Выберите значение для параметра **Если лечение невозможно**, чтобы указать действие приложения с файлом, который не удалось вылечить.
3. Настройте частоту проверки, выбрав для параметра **По расписанию** значение **Раз в неделю**, **Раз в день** или **После обновления**.

4. Укажите день и время начала проверки, выбрав значения для параметров **День запуска** и **Время запуска**.

Проверка с указанными параметрами будет запускаться согласно расписанию.

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. В панели быстрого запуска приложения Kaspersky нажмите **Сканер**.
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,

В панели быстрого запуска приложения Kaspersky нажмите **Обновление**.

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

Как запланировать автообновление

1. В главном окне приложения Kaspersky нажмите **Автоматический Антивирус**.
2. Выберите **Обновление**.
3. Нажмите **По расписанию** и выберите один из вариантов:
    - **Раз в неделю**: базы будут обновляться автоматически раз в неделю в указанные вами день и время.
    - **Раз в день**: базы будут обновляться автоматически один раз в день в указанное вами время.
    - **Выключено**: базы не будут обновляться автоматически. Вам нужно будет обновлять их вручную.
4. Чтобы указать день запуска обновления (доступно только для обновления раз в неделю), нажмите **День запуска** и выберите день.
5. Чтобы указать время запуска обновления (доступно для обновления раз в день и раз в неделю), нажмите **Время запуска** и установите время.

В данный момент мы работаем над улучшением этой функции. Изменения в ее работе - часть раннего доступа к функциям, поэтому они доступны только небольшой группе пользователей.

Автоматический Антивирус

Автоматический Антивирус осуществляет антивирусную защиту. Компонент позволяет обнаруживать и устранять вирусы, рекламные приложения и приложения, которые могут быть использованы злоумышленниками для причинения вреда вашему устройству или данным на нем.

В бесплатной версии приложения компонент называется Сканер, а в приложении, используемом по подписке, он называется Автоматический Антивирус.

Сканер

Сканер выполняет следующие функции:

- Проверка. Вы можете выбрать для проверки следующее:
  - все устройство полностью;
  - только установленные приложения;
  - выбранный файл или папку.
- Обновление. Приложение загружает обновленные антивирусные базы, которые используются при поиске угроз. Обновление обеспечивает актуальную защиту устройства.
- Карантин. Приложение помещает на карантин файлы и приложения, обнаруженные во время проверки устройства. На карантине приложение хранит файлы и приложения в запакованном виде, в котором они не могут нанести вред устройству. После того, как файл помещен в карантин, вы можете удалить его навсегда или восстановить его (приложение Kaspersky рекомендует не восстанавливать файлы из карантина, поскольку они могут повредить ваше устройство). После того, как приложение помещено в карантин, вы можете только удалить его навсегда.

  Как восстановить в исходную папку файлы, помещенные на карантин, или удалить их окончательно

  1. В главном окне приложения нажмите **Автоматический Антивирус** > **Карантин**.
  2. Нажмите на файл и выберите действие:
     - **Восстановить**: файл будет восстановлен в исходную папку.
     - **Удалить**: файл будет удален.
     - **Удалить все**: все файлы, хранящиеся на карантине, будут удалены.

В бесплатной версии вы должны запускать проверку устройства вручную.

Автоматический Антивирус

Автоматический Антивирус включает все функции Сканера и предоставляет автоматическую защиту устройства 24/7. Автоматический Антивирус позволяет обнаруживать угрозы в открытых файлах, а также проверять приложения во время их установки на устройство в режиме реального времени. Для обеспечения защиты в автоматическом режиме используются антивирусные базы и облачная служба Kaspersky Security Network.

Если на вашем устройстве установлена программа, выполняющая сбор и отправку информации на обработку, приложение Kaspersky может классифицировать такую программу как вредоносную.

Настройка параметров Автоматического Антивируса

1. В панели быстрого запуска приложения Kaspersky нажмите **Автоматический Антивирус**.
2. Нажмите **Автоматический Антивирус** и выберите режим защиты: **Рекомендуемый режим** или **Расширенный режим**.

   Расширенный режим защиты требует повышенных ресурсов энергопотребления.

3. Включите проверку на наличие рекламных приложений, а также приложений автодозвона и приложений для дистанционного управления устройством, установив флажок **Обнаружение рекламы**.

   Такая проверка позволяет обнаружить приложения, которые могут быть использованы злоумышленниками для причинения вреда пользователям.

Если вы выбрали **Расширенный режим** защиты, настройте его параметры в разделе **Настройки** > **Автоматический Антивирус**.

Если вы выбрали **Рекомендуемый режим** защиты, настройки параметров в блоке **Автоматический Антивирус** недоступны для изменения.

1. Выберите типы файлов для проверки в реальном времени: нажмите **Определенный файл или папку** и выберите значение.
2. Выберите действие приложения при обнаружении объекта во время проверки: нажмите **Действие при обнаружении** и укажите значение.

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. В панели быстрого запуска приложения Kaspersky нажмите **Где мое устройство**.

   Откроются настройки функции.

2. Нажмите **Включить** .

3. Просмотрите описание функции и нажмите **Далее**.

4. Предоставьте приложению необходимые разрешения. Эти разрешения необходимы для защиты устройства в случае кражи или потери.

5. Войдите в ваш аккаунт My Kaspersky, если вы не сделали этого ранее.

6. Настройте блокировку экрана, если вы не сделали этого ранее при настройке **Блокировка приложений**.

7. 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.

8. 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. В панели быстрого запуска приложения Kaspersky нажмите **Где мое устройство**.
2. Разблокируйте доступ к функции с помощью секретного кода, графического ключа или отпечатка пальца.

3. В разделе **Дополнительная защита** нажмите **SIM-Контроль**.

4. 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. В панели быстрого запуска приложения Kaspersky нажмите **Где мое устройство**.

2. Разблокируйте доступ к функции с помощью секретного кода, графического ключа или отпечатка пальца.

3. В разделе **Дополнительная защита** нажмите **Защита от удаления**.

4. 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 **OK**.

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.

После добавления секретного кода:

- На устройствах с Android 4.x и 5.1 системный PIN-код будет отключен.
- На устройствах с Android 5.0 приложение заменит любой системный PIN-код на PIN-код, соответствующий секретному коду для функции "Где мое устройство".

Вы можете снова задать системный PIN-код в настройках вашего устройства.

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. Нажмите  > **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** 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 **Разблокировать отпечатком пальца** в мастере первоначальной настройки или нажмите **Настройки** > **Блокировка экрана**.

Блокировка приложений

Блокировка приложений позволяет защитить ваши данные от посторонних. Вы можете защитить доступ к приложениям, содержащим ваши личные данные, например, WhatsApp, Фото, Сообщения, Snapchat, Viber, Gmail, Настройки и многим другим. Если вы открываете приложение, защищаемое Блокировкой приложений, приложение Kaspersky попросит вас разблокировать доступ к этому приложению с помощью секретного кода, графического ключа или отпечатка пальца.

Приложение Kaspersky использует настройки устройства для защиты доступа к приложениям. Чтобы обеспечить защиту, мы рекомендуем:

- защитить доступ к приложению Настройки с помощью Блокировки приложений;
- включить защиту от несанкционированного удаления приложения Kaspersky, установив флажок **Защита от удаления** в настройках функции "Где мое устройство".

Первоначальная настройка Блокировки приложений

Чтобы использовать Блокировку приложений, нужно выполнить первоначальную настройку функции и задать секретный код приложения, если вы не делали этого ранее.

Мастер первоначальной настройки Блокировки приложений запускается один раз. В дальнейшем вы можете настраивать Блокировку приложений в параметрах приложения.

Чтобы выполнить первоначальную настройку функции Блокировки приложений:

1. Откройте панель быстрого запуска приложения Kaspersky.
2. Нажмите **Блокировка приложений**.

   Запустится мастер первоначальной настройки Блокировки приложений.
3. Просмотрите описание функции и нажмите **Далее**.
4. Включите специальные возможности для приложения Kaspersky. Приложению нужны специальные возможности, чтобы блокировать приложения.

   Чтобы включить специальные возможности:

   a. На экране с информацией о специальных возможностях нажмите **Далее**.

      Откроется список приложений, установленных на вашем устройстве.

   b. Выберите в списке приложение Kaspersky.

   c. Включите соответствующий переключатель.

   d. Подтвердите операцию, нажав **ОК**.

e. Вернитесь в приложение Kaspersky.

5. В окне Блокировки приложений включите переключатель для тех приложений, которые вы хотите защитить.

6. Настройте блокировку экрана, если вы не сделали этого ранее при настройке функции "Где мое устройство" или Личных контактов.

Блокировка приложений настроена. Будет показан список приложений, защищенных секретным кодом.

Защита доступа к приложениям

Чтобы защитить доступ к приложению секретным кодом:

1. Откройте панель быстрого запуска приложения Kaspersky.

2. Нажмите **Блокировка приложений**.

3. Разблокируйте доступ к функции с помощью секретного кода, графического ключа или отпечатка пальца.

   Откроется окно настроек Блокировки приложений.

4. Найдите приложение, которое вы хотите защитить.

5. Включите соответствующий переключатель.

Теперь для доступа к защищенному приложению вам нужно вводить секретный код. Защищенные приложения отображаются в разделе **Защищенные приложения**. Если вы больше не хотите защищать доступ к приложению секретным кодом, переведите переключатель напротив этого приложения в положение ВЫКЛ.

Запуск защищенных приложений

Чтобы открыть приложение, защищенное секретным кодом:

1. Нажмите на иконку приложения на устройстве.

   Откроется окно приложения Kaspersky.

2. Разблокируйте доступ к приложению с помощью секретного кода, графического ключа или отпечатка пальца.

   Приложение откроется.

Интернет-защита

Интернет-защита проверяет сайты перед их открытием. Затем блокирует вредоносные сайты, которые распространяют вредоносный код, а также фишинговые сайты, которые крадут ваши конфиденциальные данные и могут заполучить доступ к вашим финансовым счетам.

Для получения защиты в интернете вам нужно использовать защищенный браузер (см. список защищенных браузеров).

Интернет-защита доступна только для пользователей, использующих приложение Kaspersky по подписке.

Для проверки сайтов Интернет-защита использует облачную службу Kaspersky Security Network.

Первоначальная настройка Интернет-защиты

Чтобы включить Интернет-защиту, вам нужно выполнить первоначальную настройку функции. По умолчанию после установки приложения функции Интернет-защиты выключены.

Чтобы выполнить первоначальную настройку Интернет-защиты:

1. Откройте панель быстрого запуска приложения Kaspersky.
2. Нажмите на **Интернет-защита**.

   Запустится мастер первоначальной настройки Интернет-защиты.
3. Следуйте инструкциям мастера.

   Функция "Интернет-защита" готова к использованию. Теперь вы можете безопасно открывать любые сайты, используя защищенный браузер.

Чтобы изменить параметры Интернет-защиты после первоначальной настройки:

1. Откройте приложение Kaspersky.
2. Нажмите  >**Интернет-защита**.

Поддерживаемые браузеры

Интернет-защита проверяет сайты только в браузере Google Chrome.

Интернет-защита может работать и с некоторыми предустановленными браузерами, например, с Samsung Internet на устройствах Samsung и Huawei Browser на устройствах Huawei. Другие браузеры не поддерживаются.

Если вы хотите использовать Интернет-защиту во время работы в интернете, укажите браузер Google Chrome в качестве браузера по умолчанию.

При включении Интернет-защита автоматически проверяет браузер по умолчанию. Если Google Chrome не является браузером по умолчанию, приложение предложит поменять браузер по умолчанию на Google Chrome или Huawei Browser.

Если вы не хотите менять текущий браузер по умолчанию, то запускайте браузер Google Chrome в тех случаях, когда хотите безопасно вводить персональные данные в интернете. Вы можете запустить Google Chrome из панели быстрого запуска приложения Kaspersky, нажав **Интернет-защита** > **Открыть браузер** или выбрав Chrome в меню приложений вашего устройства.

На устройствах Huawei без сервисов Google необходимо установить Huawei Browser в качестве браузера по умолчанию, чтобы использовать Интернет-защиту.

Как установить браузер по умолчанию

В этом разделе даны общие инструкции. Чтобы найти более подробную информацию, обратитесь к руководству пользователя для вашего устройства.

1. Откройте настройки устройства.
2. Нажмите **Приложения** > ⚙ > **Приложения по умолчанию**> **Браузер**.
3. Выберите Google Chrome (или Huawei Browser на устройстве Huawei без сервисов Google).

   Теперь Google Chrome или Huawei Browser ваш браузер по умолчанию. Вы можете использовать Интернет-защиту и включить функцию проверки ссылок, которые вы открываете внутри приложений.

Фильтрация контента в Японии

Функция Веб-контроль доступна в приложении только на территории Японии, чтобы соответствовать японскому законодательству.

Функция Веб-контроль доступна только при использовании приложения Kaspersky по подписке.

Веб-контроль позволяет управлять веб-контентом на мобильном устройстве и защищать от нежелательного онлайн-контента. Например, вы можете установить приложение Kaspersky на устройство вашего ребенка и выбрать, какие категории контента и конкретные сайты будут доступны ему или ей.

Для получения защиты в интернете вам нужно использовать защищенный браузер (см. список защищенных браузеров).

Чтобы настроить веб-контроль,

1. На детском устройстве откройте приложение Kaspersky.
2. На панели быстрого запуска нажмите **Интернет-защита**.
3. Нажмите **Настройки**на экране **Браузер с защитой**.
4. Нажмите **Настроить Веб-контроль** и задайте пароль, секретный вопрос и ответ, чтобы убедиться, что только взрослый может изменять эти настройки функций.
5. Нажмите **Режим** на экране **Настройка Веб-контроля** и установите ограничения по возрасту. Если вы выберете **Специальный**, вы можете вручную заблокировать доступ к определенным категориям веб-сайтов.
6. Вернитесь к экрану **Интернет-защита**.

Веб-контроль настроен.

При необходимости вы можете добавить сайты в список исключений. Веб-контроль не блокирует веб-сайты, добавленные в список исключений, даже если они принадлежат к запрещенным категориям.

Чтобы исключить определенные веб-сайты,

1. На панели быстрого запуска нажмите **Интернет-защита**.
2. Нажмите **Настройки** на экране **Браузер с защитой**.
3. Нажмите **Настроить Веб-контроль** и введите пароль.
4. Нажмите **Исключения** на экране **Защищенный браузер**.
5. Нажмите **Добавить веб-адреса** и введите адрес веб-сайта. Доступ ко всем веб-страницам с указанного сайта будет разрешен.

   Если вы хотите разрешить доступ только к одной веб-странице, введите ее адрес и установите флажок **Разрешить доступ только к этой странице этого веб-сайта** .
6. Нажмите **Сохранить**.
7. Вернитесь к экрану **Интернет-защита**.

Защита чатов

О Защите чатов

Функция Защита чатов проверяет полученные SMS-сообщения и сообщения в мессенджерах на наличие фишинговых ссылок.

Функция "Защита чатов" доступна только при использовании приложения Kaspersky по подписке.

Защита чатов использует Kaspersky Security Network для проверки ссылок в сообщениях.

Защита чатов блокирует ссылки только в Google Chrome. Чтобы защитить себя от опасных ссылок в мессенджерах, установите Google Chrome в качестве браузера по умолчанию .

Интернет-защита может работать и с некоторыми предустановленными браузерами, например, с Samsung Internet на устройствах Samsung. Другие браузеры не поддерживаются. Если у вас есть устройство Huawei без браузера Google Chrome, эта функция вам недоступна. В этом случае ограниченная функциональность Защиты чатов доступна как SMS Анти-Фишинг.

Проверка ссылок в SMS-сообщениях

Если вы получите SMS-сообщение, содержащее ссылки на вредоносные или поддельные веб-сайты, приложение уведомит вас об этом. Вам остается решить, хотите ли вы все же переходить по ссылке.

Чтобы проверять ссылки в SMS-сообщениях:

1. В главном окне приложения Kaspersky в панели быстрого запуска нажмите **Защита чатов**.
2. Нажмите **Проверка ссылок в СМС**.
3. Установите переключатель **Предупреждать об опасных ссылках** в положение ВКЛ.

   Приложение Kaspersky уведомит вас, если полученное вами SMS-сообщение содержит ссылки на вредоносные или поддельные веб-сайты.

Проверка ссылок в мессенджерах

Защита чатов проверяет ссылки, которые вы получаете в сообщениях через мессенджеры WhatsApp, Viber, Telegram и Google Hangouts.

Если в полученном вами сообщении содержится ссылка на вредоносный или поддельный веб-сайт, приложение заблокирует эту ссылку и покажет вам окно предупреждения в браузере.

Защита чатов блокирует ссылки только в Google Chrome. Чтобы защитить себя от опасных ссылок в мессенджерах, установите Google Chrome в качестве браузера по умолчанию .

Интернет-защита может работать и с некоторыми предустановленными браузерами, например, с Samsung Internet на устройствах Samsung. Другие браузеры не поддерживаются.

Чтобы включить блокировку опасных ссылок, полученных в мессенджерах:

1. В главном окне приложения Kaspersky в панели быстрого запуска нажмите **Защита чатов**.
2. Нажмите **Проверка ссылок в мессенджерах**.
3. Установите переключатель **Блокировать опасные ссылки** в положение ВКЛ.

   Приложение Kaspersky заблокирует ссылки на вредоносные или поддельные веб-сайты, которые вы получите в сообщениях через мессенджеры.

SMS Анти-Фишинг (для Huawei устройств без сервисов Google Play)

Функция SMS Анти-Фишинг пришлет уведомление, если вы получите SMS-сообщение, содержащее ссылки на вредоносные и поддельные веб-сайты.

Эта функция доступна только для устройств Huawei без браузера Google Chrome. На устройствах с браузером Google Chrome доступна расширенная версия этой функции (см. Защита чатов).

SMS Анти-Фишинг доступен только при использовании приложения Kaspersky по подписке.

SMS Анти-Фишинг использует Kaspersky Security Network для проверки ссылок в SMS-сообщениях.

Чтобы проверять ссылки в SMS-сообщениях:

1. В главном окне приложения Kaspersky в панели быстрого запуска нажмите **SMS Анти-Фишинг**.
2. Установите переключатель **SMS Анти-Фишинг** в положение ВКЛ.

   Функция SMS Анти-Фишинг включена.

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, вы можете помочь "Лаборатории Касперского" 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.

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 9-12, 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. В панели быстрого запуска приложения Kaspersky нажмите **Фильтр звонков**.
2. В блоке **Запрещенные номера** нажмите +.
3. Укажите информацию для запрещенного контакта.
4. Нажмите ✓, чтобы сохранить введенный номер.

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 **Уведомлять после звонка** включена, приложение предложит вам заблокировать этот номер после звонка.

В окне подсказки выберите одно из следующих действий:

- **Блокировать**, 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. В панели быстрого запуска приложения Kaspersky нажмите **Фильтр звонков**.
2. В блоке **Запрещенные номера** выберите контакт, который вы хотите изменить.
3. Измените данные контакта.
4. Нажмите ✓, чтобы сохранить введенный номер.

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

Как удалить контакт из списка запрещенных номеров?

1. В панели быстрого запуска приложения Kaspersky нажмите **Фильтр звонков**.

2. В блоке **Запрещенные номера** выполните одно из следующих действий:

   - Смахните контакт влево и нажмите .
   - Выберите контакт, который вы хотите удалить из списка, и нажмите **Удалить контакт**.

3. 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 панели быстрого запуска приложения Kaspersky нажмите **Фильтр звонков**.
2. 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** недоступна на устройствах под управлением операционной системы Android 9-12.

Чтобы включить подсказку:

1. В панели быстрого запуска приложения Kaspersky нажмите **Фильтр звонков**.
2. 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. Обращаем внимание, что приложение Kaspersky Who Calls доступно только в России.

Мои приложения и разрешения

О функции "Мои приложения"

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

Эта функция доступна только на устройствах с Android 5.0–12.

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. В панели быстрого запуска приложения Kaspersky нажмите **Мои приложения**.
2. Перейдите в раздел **Приложения**.
3. 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 **Разрешите доступ к использованию**.

d. Вернитесь в приложение Kaspersky.

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

Просмотр установленных приложений

1. В панели быстрого запуска 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 панели быстрого запуска 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 панели быстрого запуска 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.

Приложение Kaspersky проверяет аккаунты по базе, предоставленной сайтом www.haveibeenpwned.com. Если при проверке будет обнаружено, что ваши данные могли попасть в публичный доступ, приложение уведомит вас об этом и покажет список сайтов, с которых могла произойти утечка данных, даты возможной утечки и категории данных, которые могли попасть в публичный доступ.

Используя 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 **Поиск 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

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 ограниченную 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.

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.

Ограниченная версия Kaspersky Secure Connection

Вы можете использовать ограниченную или премиум-версию 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 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.

Премиум-версия 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 использовании *платной 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 премиум-версию вам нужно оформить подписку на безопасное VPN-соединение. Вы можете оформить или продлить подписку в приложении.

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

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

Чтобы посмотреть состояние безопасного 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 премиум-версии безопасного VPN-соединения

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

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

Чтобы перейти на безлимитную версию:

1. Перейдите в раздел безопасного VPN-соединения.
2. В нижней части экрана нажмите **Перейти на Премиум**.

   Пролистайте экраны с описанием функций и выберите Премиум.
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 Kaspersky Secure Connection.

   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 расширенную 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 **Умная защита** 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 **Банковские сайты**, 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 9–12.x 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 "Устройства в моей сети" 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:

   - **Банковские сайты**.
   - **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 **Для незащищенных сетей 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:

   - **Как 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 ограниченной 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 VPN

Запрещается использование программы Kaspersky Secure Connection в следующих целях:

- Нарушение любого применимого местного, национального или международного законодательства или регулирования той страны, где находится VPN-сервер или

используется программа.

- Ппричинение вреда или попытки причинения вреда несовершеннолетним любым способом.

- Использование программы недолжным образом и намеренное внедрение вредоносных компьютерных программ или любых других подобных фрагментов кода, которые являются вредоносными и / или приносят технологический ущерб.

- Проведение реверс-инжиниринга, декомпиляции, дизассемблирования, модификации, интерпретации, а также любых попыток раскрыть исходный код программы или создания производных работ.

- Получение несанкционированного доступа, вмешательство, нанесение ущерба или повреждение программы. Любое нарушение такого рода будет передано соответствующему полномочному органу исполнительной власти, и мы будем содействовать этим органам для раскрытия вашей личности. В случае такого нарушения действие ваших прав на использование программы будет немедленно прекращено;

- Загрузка, публикация, отправка по электронной почте или передача иным способом любого контента, который направлен на провокацию поведения, которое является незаконным, опасным, угрожающим, насильственным, направленным на домогательство, нечестным, дискредитирующим, аморальным, непристойным, клеветническим, посягающим на неприкосновенность частной жизни, злонамеренным или расистским, вызывающим этнические или иные конфликты, и возможно провоцирующим такое поведение.

- Выдача себя за любое другое физическое или юридическое лицо или искажение иным способом своей принадлежности к физическому или юридическому лицу в случаях, когда такая идентификация требуется или предусмотрена применимым законодательством.

- Фальсификация или манипуляция идентификаторами с целью сокрытия первоисточника любого контента, передаваемого по системам VPN.

- Загрузка, публикация, отправка по электронной почте или передача иным способом любого контента, который нарушает права на любой патент, товарный знак, коммерческую тайну, авторское право или другую интеллектуальную собственность какой-либо стороны.

- Загрузка, публикация, отправка по электронной почте или передача иным способом любых нежелательных или несанкционированных объявлений, рекламных материалов, например, "нежелательной почты", "спама", "писем счастья", или "пирамидных схем".

- Вмешательство или выведение из строя систем VPN, и /или VPN-серверов, и / или VPN-сетей, или нарушение любых требований, процедур, политик или правил сетей, подключенных к системам VPN.

- Сбор и хранение персональных данных других пользователей без их ведома.
- Распространение побуждающей к действию информации о нелегальной деятельности, а также содействие нанесению физического ущерба или травм любой группе людей или отдельным личностям или содействия любого акта насилия над животными.

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

Устройства в моей сети

Эта функция доступна только в приложении Kaspersky Plus и Premium.

Мы улучшили работу функции на версиях Android 11-12.x. Теперь вы можете пользоваться функцией «Устройства в моей сети» без ограничений.

Функция "Устройства в моей сети" показывает устройства, которые подключены к вашей домашней сети Wi-Fi. С помощью этой функции вы можете предотвратить подключение к вашей сети неавторизованных устройств и проверить состояние защиты устройств, подключенных к сети.

К сети Wi-Fi может быть подключено несколько устройств. Подобрав пароль или взломав доступ к вашей домашней сети, злоумышленники могут воспользоваться вашим интернетом или получить доступ к вашим данным. С помощью приложения Kaspersky вы можете своевременно узнавать о подключении к вашей домашней сети Wi-Fi новых устройств.

Когда ваше устройство подключается к сети Wi-Fi, приложение Kaspersky спрашивает, хотите ли вы посмотреть другие устройства, подключенные к этой сети. Если вы соглашаетесь, отображается список устройств, подключенных к этой сети и уведомление при подключении нового устройства. Таким образом, вы можете контролировать вашу домашнюю сеть Wi-Fi и защищать все подключенные устройства и данные.

Даже одно незащищенное устройство в сети Wi-Fi снижает защиту других устройств. С помощью приложения Kaspersky вы можете перейти на сайт My Kaspersky и установить приложения "Лаборатории Касперского" на все ваши устройства для их защиты.

Чтобы установить приложение Kaspersky на другом устройстве (если вы приобрели подписку на несколько устройств):

1. Нажмите на **Устройства в моей сети** на главном экране приложения, затем нажмите на название устройства, с которым вы хотите поделиться своей подпиской.

   Откроется окно с информацией об этом устройстве.

2. В разделе **В вашей подписке** нажмите на приложение Kaspersky.

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

   Отобразится системное окно с вариантами, как можно поделиться ссылкой.

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

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

Если к сети Wi-Fi, проверяемой приложением Kaspersky, подключено более тысячи устройств, приложение может работать с задержками. Специалисты "Лаборатории Касперского" не рекомендуют использовать приложение для общественных сетей Wi-Fi.

Включение функции "Устройства в моей сети"

Чтобы включить контроль устройств, подключенных к вашей домашней сети Wi-Fi, выполните следующие действия:

1. Подключитесь к вашей домашней сети Wi-Fi.

2. Откройте приложение Kaspersky.

3. Нажмите на раздел **Устройства в моей сети** на главном экране приложения.

4. Следуйте инструкции в разделе **Устройства в моей сети**, чтобы включить функцию.

   Приложение выполнит проверку сети и покажет список подключенных устройств, а также информацию об этих устройствах.

Без доступа к вашей геолокации функция "Устройства в моей сети" 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.

Выключение функции "Устройства в моей сети"

Чтобы выключить контроль устройств, подключенных к вашей домашней сети Wi-Fi, выполните следующие действия:

1. Откройте приложение Kaspersky.
2. Нажмите на раздел **Устройства в моей сети** на главном экране приложения.

   Откроется раздел **Устройства в моей сети**.
3. Нажмите  >**Забыть эту сеть Wi-Fi** в верхней части экрана.
4. Подтвердите действие.

Приложение не будет показывать устройства, подключенные к вашей сети.

Вы можете также отключить контроль устройств в сети, отклонив **Положение об обработке данных для обеспечения функциональности "Устройства в моей сети"**. Если вы отклоните Положение, функция "Устройства в моей сети" будет отключена на вашем устройстве, а все настройки функции будут сброшены.

Если вы захотите снова включить функцию, вы можете это сделать в разделе Устройства в моей сети на главном экране приложения.

Просмотр устройств в вашей сети

Компонент Устройства в моей сети позволяет выполнять следующие действия:

- Просмотреть и настроить список устройств, подключенных к вашей домашней сети Wi-Fi. Вы можете изменить тип и имя устройств из списка.

В разделе **Устройства в моей сети** вы можете просмотреть следующую информацию:

- Устройства, подключенные к сети Wi-Fi в данный момент.
- Устройства, которые были подключены к сети Wi-Fi какое-то время назад.
- Статус устройств в сети Wi-Fi (новые устройства, подключенные устройства и отключенные устройства).

- Время последнего обнаружения отключенных устройств в сети.

Когда новое устройство подключается к сети Wi-Fi, приложение Kaspersky отображает следующую информацию об устройстве:

- имя устройства (если доступно);
- производитель устройства;
- тип устройства (например: компьютер, мобильное устройства, роутер, игровая консоль или видеокамера);
- операционная система, установленная на устройстве;
- MAC-адрес (уникальный сетевой идентификатор устройства);
- IP-адрес устройства.

Чтобы просмотреть устройства, подключенные к домашней сети Wi-Fi, выполните следующие действия:

1. Подключитесь к вашей домашней сети Wi-Fi.
2. Откройте приложение Kaspersky.
3. Нажмите на раздел **Устройства в моей сети** на главном экране приложения.

   Откроется раздел **Устройства в моей сети**.
4. При необходимости подтвердите, что это ваша домашняя сеть Wi-Fi.

Что делать, если неизвестное устройство подключается к домашней сети Wi-Fi

Если новое устройство подключается к вашей домашней сети Wi-Fi, можно выполнить следующее действие:

Если вы не знаете, кто использует новое устройство, вы можете нажать на **Читать советы** в разделе **Как защитить ваш домашний Wi-Fi?**, чтобы узнать, что делать в таких случаях. В результате вы перейдете в Базу знаний "Лаборатории Касперского", где можно узнать, как защитить домашнюю сеть Wi-Fi от непрошеных гостей.

Менеджер паролей

О компоненте Менеджер паролей

Kaspersky Password Manager доступен только в Kaspersky Plus и Premium.

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

Работу компонента Менеджер паролей обеспечивает приложение Kaspersky Password Manager. Вам нужно установить Kaspersky Password Manager после установки основного приложения Kaspersky, чтобы использовать функцию менеджера паролей.

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

Установка и запуск Kaspersky Password Manager

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

1. Откройте приложение Kaspersky.
2. В разделе **Менеджер паролей** нажмите **Загрузить и установить**.

   Откроется страница с информацией о Kaspersky Password Manager.
3. На странице с информацией о приложении нажмите **Установить**.
4. Ознакомьтесь со списком прав, которые нужны приложению Kaspersky Internet Security:

   - Если вы согласны предоставить приложению эти права, нажмите **Принять**.

     Начнется загрузка и установка приложения Kaspersky Password Manager.
   - Если вы не согласны предоставить приложению Kaspersky Password Manager эти права, нажмите **Назад.**

     В этом случае установка приложения будет отменена.

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

1. Откройте приложение Kaspersky.
2. В разделе **Менеджер паролей** нажмите **Открыть**.
3. Откроется окно приложения Kaspersky Password Manager.

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

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 небезопасные 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. Нажмите на раздел **Поиск небезопасных настроек**, чтобы открыть его.

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.

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.

QR-сканер

Работу этого компонента обеспечивает приложение Kaspersky QR Scanner. Kaspersky QR Scanner позволяет сканировать QR-коды и получать доступ к зашифрованной них информации. При доступе выполняется проверка ссылок, содержащихся в QR-коде.

Приложение Kaspersky QR Scanner бесплатное. Вы можете установить его из Google Play. Kaspersky QR Scanner не отображается в меню приложения после установки.

Управление моей приватностью

Управление моей приватностью

> Эта функция доступна только в Kaspersky Plus и Premium.

Популярные сервисы, такие как Google, собирают ваши данные, когда вы их используете. Эта информация используется, чтобы персонализировать результаты ваших поисковых запросов и взаимодействие с другими пользователями. Мы считаем, что у вас должна быть возможность посмотреть, какие данные собирает сервис, а также перестать передавать эти данные приложению или делиться с другими пользователями тогда, когда захотите. Функциональность "Управление моей приватностью" позволяет вам управлять сбором ваших данных и настройками приватности в разных сервисах — прямо из нашего приложения. Контролируйте сбор ваших данных и узнавайте, как защитить свою приватность при использовании интернет-сервисов.

Как это работает

Чтобы начать использование функции "Управление моей приватностью", примите **Положении** во время прохождения мастера первого запуска или позже, когда решите использовать функцию. Это применимо, если вы используете приложение Kaspersky в Европейском Союзе. Вы можете отменить свое решение в любое время, но отзыв согласия с положением приведет к ограничению функциональности "Управления моей приватностью".

Ниже приведена таблица, показывающая, какие сервисы сейчас поддерживает функция и сбор каких данных вы можете посмотреть и настроить.

Сервис	Настраиваемые данные
Google	• **История поиска** (Google, YouTube) • **История посещенных сайтов и просмотров** (Google, YouTube) • **История посещенных мест** (Google Maps)

Для каждого типа данных вы можете управлять настройками приватности в более детализированном виде.

В рамках этой функциональности, помимо управления сбором данных, вы можете ознакомиться с полезными статьями о приватности в интернете. Чтобы прочитать статью, нажмите на ее название в разделе **Станьте экспертом в вопросах конфиденциальности** на главном экране функции.

Управление сбором данных и настройками приватности

Функция "Управление моей приватностью" позволяет узнать, какие из ваших персональных данных собирает Google, очистить историю поиска и отключить сбор данных.

Управление ваше историей поиска в Google

1. На главном экране функции "Управление моей приватностью" перейдите в раздел **Сервисы** и нажмите на **Google**. Войдите в вашу учетную запись Google, если это потребуется.
2. В разделе **История** нажмите на тот тип истории ваших действий, о котором хотите узнать больше.
3. Если вы хотите очистить историю, собранную Google, вернитесь в секцию **Google**, а затем, в секции **История**, нажмите **Управлять историей**.
4. На открывшемся экране выберите историю действий, которую вы хотите удалить. Затем нажмите **Удалить**.

   Собранная история будет удалена. Если вы не хотите, чтобы Google собирал ваши личные данные, отключить сбор данных в разделе **Сбор данных** на главном экране Google функции "Управление моей приватностью". Если этого не сделать, новая история действий, собранная Google, будет появляться в разделе **История** функции "Управление моей приватностью".

Управление сбором ваших данных в Google

1. На главном экране функции "Управление моей приватностью" перейдите в раздел **Сервисы** и нажмите на **Google**. Войдите в вашу учетную запись Google, если это потребуется.

2. В разделе **Сбор данных** нажмите **Управлять сбором данных**.

3. Выберите сервис, с которым вы больше не хотите делиться своими данными, и нажмите **Остановить отслеживание**.

4. Если вы хотите остановить сбор данных для всех сервисов, вернитесь в раздел **Сбор данных** и нажмите на **Управлять сбором данных**.

5. На открывшемся экране выберите сервисы, с которыми вы не хотите больше делиться данными, и нажмите **Остановить отслеживание**.

   Сервисы Google больше не будут собирать ваши данные, но история ваших действий не будет удалена. Если вы хотите удалить историю действий, удалите собранные данные в разделе **История** на главном экране Google функции "Управление моей приватностью".

Если вы отключите сбор данных для приложений и веб-поиска, персонализация ваших сервисов Google может быть ограничена. Например, Google может перестать рекомендовать места, которые могут быть вам интересны, а также результаты вашего веб-поиска могут стать менее релевантными. Сбор данных будет остановлен во всех приложений, на всех сайтах и устройствах, где вы выполнили вход в одну учетную запись. После того, как вы остановите сбор данных, Google еще может некоторое время использовать собранную информацию ваших недавних веб-запросов, чтобы улучшать выдачу при новых запросах во время активной сессии. Отключение сбора данных не приводит к удалению всей ранее собранной информации. Вы можете посмотреть и удалить эту и другую информацию на сайте myactivity.google.com. Перейдите на сайт policies.google.com, чтобы узнать больше о том, какие данные Google продолжит собирать и почему.

В будущем мы планируем подключить возможность настраивать сбор данных и управлять своей приватностью и для других сервисов.

Ответы на часто задаваемые вопросы

Здесь собраны ответы на некоторые из часто задаваемых вопросов о функции "Управление моей приватностью".

Как мне отключить контекстную рекламу в сервисах Google?

1. На главном экране функции "Управление моей приватностью" перейдите в раздел **Сервисы** и нажмите на **Google**. Войдите в вашу учетную запись Google, если это потребуется.

2. В разделе **История** нажмите на **Управлять историей**.

3. На следующем экране убедитесь, что установлены все флажки, а затем нажмите **Удалить**.

4. Вернитесь на главный экран **Google** функции "Управление моей приватностью".

5. В разделе **Сбор данных** нажмите на **Управлять сбором данных**.

6. На следующем экране убедитесь, что установлены все флажки, а затем нажмите **Остановить отслеживание**.

Как спрятать мое местоположение от Google?

1. На главном экране функции "Управление моей приватностью" перейдите в раздел **Сервисы** и нажмите на **Google**. Войдите в вашу учетную запись Google, если это потребуется.

2. В разделе **История** нажмите на **Управлять историей**.

3. В разделе **Google Карты** поставьте флажок для **История посещенных мест**. Убедитесь, что все остальные флажки не проставлены, если вы не хотите удалить остальные категории истории ваших действий.

4. Нажмите **Удалить**.

5. Вернитесь на главный экран **Google** функции "Управление моей приватностью".

6. В разделе **Сбор данных** нажмите на **Управлять сбором данных**.

7. В разделе **Google Карты** поставьте флажок для **Местоположение**. Убедитесь, что все остальные флажки не проставлены, если вы не хотите удалить остальные категории сбора данных.

8. Нажмите **Остановить отслеживание**.

Kaspersky Premium включает в себя защиту от кражи личных данных, предоставляемую Iris Powered by Generali — международной компанией, занимающейся защитой персональных данных и кибербезопасностью. Защита от кражи личных данных доступна не во всех странах.

Проверьте, доступна ли защита от кражи личных данных в вашей стране.

Помощь в случае кражи личных данных

Помощь в случае кражи личных данных доступна по телефону не во всех регионах.

Специалисты колл-центра разрешения проблем доступны круглосуточно и без выходных, чтобы помочь восстановить вашу утерянную личность и предотвратить дальнейший ущерб в случае инцидента:

- Помощь при утере/краже кошелька. Мы поможем вам сделать запрос в соответствующий банк или орган, выдавший карту, об аннулировании и замене украденных или недостающих предметов, таких как ваша дебетовая/кредитная карта, водительские права, карта социального страхования или паспорт.

- Сокращение предварительно утвержденных кредитных предложений. Наша служба отказа от предложений помогает защитить вашу конфиденциальность, сокращая количество предварительно одобренных предложений по кредитным картам, некоторые из которых могут быть отправлены мошенниками для кражи вашей личной информации.

- Удаление из списков телемаркетинга. Наша служба отказа от предложений помогает вам сократить количество предложений прямой почтовой рассылки по кредитным картам и маркетинговых телефонных звонков, некоторые из которых могут быть организованы мошенниками для кражи вашей личной информации.

- Размещение предупреждений о мошенничестве в интернете. Если ваши личные данные находится под угрозой, вы можете поместить предупреждение о мошенничестве сроком на один год в свой кредитный файл, что затруднит для преступников открытие нового кредита на ваше имя без вашего ведома.

- Полностью управляемое восстановление утерянных документов и бумаг. Если вы или близкий человек, включенные в ваш тарифный план, станете жертвой кражи личных данных или мошенничества, специальный специалист по разрешению проблем займется восстановлением ваших личных данных (после заполнения и подачи полицейского отчета, ограниченной доверенности и аффидевита о краже личных данных) . Обратите внимание: доступность этой функции зависит от страны и местного законодательства.

- Уведомление кредитора, споры и последующие действия. В тех странах, где это возможно, мы свяжемся с отделами по борьбе с мошенничеством ваших кредиторов, предоставив отдельные детализированные выписки по счетам, чтобы оспорить каждый случай мошенничества. Мы будем следить за ведением этих дел до тех пор, пока каждый вопрос не будет полностью решен, информируя вас на протяжении всего процесса с помощью регулярных отчетов.

- Обращение в полицию и судебные органы. Мы поможем вам уведомить местные органы власти о мошеннической деятельности и направим отчет о мошеннической деятельности

кредиторам.

- Помощь при краже медицинских данных. В тех странах, где это возможно, мы предоставим помощь в случае, если вы станете жертвой кражи медицинских данных, с мошенническими медицинскими заявлениями, оформленными на ваше имя, и медицинской помощью, которая была получена другим лицом от вашего имени обманным путем. Мы поможем вам обеспечить исправление медицинских и страховых требований и медицинских записей и при необходимости привлечем наш штатный медицинский персонал.

- Организация поездок и путешествий. Если вы столкнулись с кражей личных данных во время путешествия на расстояние более 100 миль от дома, мы поможем с экстренными мерами во время поездки, включая бронирование авиабилетов, гостиниц и проката автомобилей.

- Срочная выдача наличных. Если вы столкнулись с кражей личных данных на расстоянии более 100 миль от вашего основного места жительства, мы предоставим вам экстренный аванс наличными в размере до 500 долларов США. Все расходы, связанные с этой услугой, будут вашей ответственностью. Эти услуги должны быть обеспечены действующей кредитной картой. Любой аванс, сделанный вам, не обеспеченный действующей кредитной картой и выплаченный GGA компанией-эмитентом кредитной карты в течение 30 дней после такого аванса, должен быть возмещен вами в течение 45 дней с даты такого аванса. После этого на любую причитающуюся сумму будут начисляться проценты по ставке 1,5% в месяц. Невзирая на положения настоящего документа об обратном, GGA не несет никаких обязательств по авансированию средств, не обеспеченных действующей кредитной картой.

> Доступность вышеупомянутых услуг зависит от страны.

Страхование от кражи личных данных

С помощью страхования от кражи личных данных вы можете защитить себя от финансового ущерба, связанного с раскрытием и восстановлением украденных личных данных. Обеспечьте себе душевное спокойствие благодаря полису страхования от кражи личных данных на сумму 1 миллион долларов США для возмещения расходов на восстановление данных.

Страхование от кражи личных данных предоставляется в соответствии с генеральным полисом страхования, подписанным отделением Generali в США, который был выдан Generali Global Assistance, Inc. Это краткое изложение предназначено только для информационных целей и не включает все положения, условия и исключения политики. Покрытие может быть доступно не во всех юрисдикциях. Пользователи должны обратиться к фактической политике для ознакомления с положениями, условиями и исключениями покрытия. Участники также должны ознакомиться с кратким описание преимуществ. Филиал Generali в США (Нью-Йорк, штат Нью-Йорк; NAIC № 11231) работает под следующими названиями: Generali Assicurazioni Generali S.P.A. (U.S. Branch) in California, Assicurazioni Generali – U.S. Branch in Colorado, Generali U.S. Branch DBA The General Insurance Company of Trieste & Venice in Oregon и The General Insurance Company of Trieste and Venice – U.S. Branch in Virginia. Филиал Generali в США допущен или имеет лицензию на ведение бизнеса во всех штатах и округе Колумбия.

Доступность вышеупомянутых услуг зависит от страны.

Предотвращение мошенничества и помощь в случае произошедшего мошенничества

Мошенники используют самые разные пути, чтобы украсть ваши деньги. Они могут прислать вам поддельные счета или попросить вас оплатить поддельные онлайн-заказы. Если у вас возникнут сомнения в достоверности того или иного предложения, вы можете позвонить нам, и мы проверим его для вас.

Предотвращение мошенничества и помощь включают в себя:

- ScamAssist. Если вы получили сообщение или предложение, которое вызывает тревогу или кажется слишком хорошим, чтобы быть правдой, наши специалисты из ScamAssist проанализируют это сообщение и предупредят вас, если оно похоже на мошенничество, помогая снизить вероятность того, что киберпреступник украдет ваши деньги или конфиденциальную информацию.

Поставщик услуг не несет ответственности за доступность, безопасность, точность или эффективность методов, продуктов, инструментов или ресурсов, используемых поставщиком услуг в его службе предотвращения мошенничества и помощи, и ваш доступ и использование службы предотвращения мошенничества и помощи происходят исключительно на ваш собственный страх и риск.

Премиальная техническая поддержка

Службы поддержки Kaspersky Premium доступны по телефону не во всех регионах.

С услугами премиальной технической поддержки Kaspersky вы получаете дополнительную защиту и удобство, в том числе, приоритетный доступ, экспертные услуги по установке, проверку и удаление вирусов, а также проверку работоспособности ПК. Премиальная техническая поддержка Kaspersky доступна не во всех странах.

Экспертные услуги по установке

Всякий раз, когда у вас возникает проблема с установкой на вашем компьютере, вы можете позвонить нам, и эксперт «Лаборатории Касперского» удаленно:

- запустит установку через удаленное подключение.
- убедится, что процесс установки проходит без ошибок.
- предоставит обзор настроек и функций приложения.
- ответит на любые вопросы о приложении или установке в процессе.
- настроит параметры приложения в соответствии с вашими потребностями.
- убедится, что приложение установлено, правильно настроено и работает правильно.

Приоритетный доступ к поддержке премиум-класса

Приоритетный доступ к поддержке премиум-класса по телефону или в чате. Телефонные звонки клиента имеют наивысший приоритет (принимаются без очереди), а предоставляемая программа чата включает возможности удаленной помощи.

Поддержка удаленного доступа

Доступ одним щелчком мыши к чату с специалистом поддержки премиум-класса с неограниченным объемом удаленной помощи. Устройтесь поудобнее и расслабьтесь, а мы все исправим!

Проверка и удаление вирусов

Профессиональное удаление вирусов и шпионских программ на любом устройстве Windows с установленной программой Kaspersky.

Проверка работоспособности ПК

Во время проверки работоспособности наши специалисты проведут многоточечный осмотр, чтобы обеспечить высочайший уровень защиты и производительности устройства.

> Чтобы воспользоваться премиальной технической поддержкой Kaspersky , позвоните по номеру телефона, привязанному к стране, в которой вы приобрели подписку на Kaspersky Premium.

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  .
2. Выберите **Настройки**.
3. Нажмите **Отчеты**.

Использование My Kaspersky

О сайте My Kaspersky

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

- удаленного управления работой некоторых программ "Лаборатории Касперского" на устройствах;

- загрузки установочных пакетов программ "Лаборатории Касперского" на устройства;

Можно войти на сайт My Kaspersky одним из следующих способов:

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

Для начала работы необходимо подключить ваши устройства к My Kaspersky.

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

Об аккаунте My Kaspersky

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

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

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

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

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

Активируйте аккаунт по ссылке из сообщения.

О двухэтапной проверке

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

Двухэтапная проверка не позволит злоумышленникам войти в ваш аккаунт My Kaspersky, даже если им известен пароль. Для подтверждения вашей личности вам 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 сайте My Kaspersky. Если вы поменяли свой номер телефона, его можно обновить на сайте My Kaspersky. Если вы вошли в аккаунт на устройстве до настройки двухэтапной проверки, ничего не изменится. Более подробная информация приведена в справке My Kaspersky.

У кода безопасности короткий срок действия. Если срок его действия истек, запросите новый код безопасности.

Если вы не получили SMS с кодом безопасности

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

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

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 панели навигации слева в приложении 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 главном экране приложения нажмите  .
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. Нажмите  > **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 к программе или в других источниках информации о программе, 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 технической 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" в сообществе

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

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

Известные проблемы

Некоторые проблемы относятся только к функциям, доступным по подписке.

Общие проблемы

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

Для приложения Kaspersky известны следующие проблемы:

- Функция "Безопасное VPN-соединение" не работает в приложении Kaspersky, если эта же функция работает в Kaspersky Security Cloud или Kaspersky Secure Connection на том же устройстве. В таком случае, если вы хотите использовать эту функцию в приложении Kaspersky, вам нужно перенести настройки безопасного VPN-соединения из другого приложения в приложение Kaspersky.

- Функция "Устройства в моей сети" не работает в приложении Kaspersky, если эта же функция работает в Kaspersky Security Cloud.

- На некоторых устройствах "Блокировка приложений" может работать неправильно в режиме разделенного экрана.

- Если вы заблокируете камеру в панели быстрых настроек устройства на Android 12, вы не сможете сделать тайное фото с помощью функции "Где мое устройство".

- На устройствах с операционной системой Android 11 и 12 не работает функция защиты от удаления приложения. Это связано с требованиями Google.

- На устройствах с операционной системой Android 6 если вы копируете вредоносное ПО в диспетчере файлов, Автоматический Антивирус не обнаруживает его. Это происходит из-за известной проблемы Android 6. По этой причине приложение не может отслеживать изменения в файловой системе устройства. Если вы запустите проверку устройства, приложение найдет это вредоносное ПО. Рекомендуем обновить прошивку или регулярно запускать проверку устройства.

- На устройствах с Android версии 5.1 или более ранней и несколькими SIM-картами приложение может не определять телефонные звонки на одну из SIM-карт. Это вызвано техническими ограничениями Android 5.1 и более ранних версий.

- Компонент "Мои приложения" не работает должным образом на устройствах с версией операционной системы ниже Android 5.

- Приложение Kaspersky не блокирует входящие спам-звонки на второй линии.

- На некоторых устройствах с кастомными прошивками MIUI и EMUI "Защита от удаления" может не работать в приложении Kaspersky. Это вызвано техническими ограничениями прошивки. Мы рекомендуем вам регулярно устанавливать обновления прошивки, так как обновления могут включать исправления проблем, влияющих на работу функции Защиты от удаления.

- Функция Фильтр звонков может не блокировать вызовы с номера, который попадает в интервал, указанный в списке запрещенных номеров. Начиная с версии 11.20.4.x, приложение не поддерживает блокировку по интервалам номеров.

- Из-за технических ограничений в Android 5.x функции "Интернет-защита" и "Защита чатов" могут не сработать, если вы открываете вредоносную или фишинговую ссылку в Google Chrome с помощью функции "Открыть ссылку в новой вкладке" в контекстном меню. Мы рекомендуем не открывать ссылки таким образом на устройствах с Android 5.x.

- На некоторых устройствах при блокировании приложений с помощью функции "Блокировка приложений" вам может быть недоступна разблокировка приложения отпечатком пальца. Мы работаем над исправлением этой проблемы. На данный момент рекомендуется разблокировать приложения с помощью секретного кода или графического ключа. Эта проблема зарегистрирована на некоторых устройствах с обновлением системы безопасности от 1 января 2021 года.

- На устройствах с подпиской на приложение Kaspersky, если вы скачали обновление безопасности Google от 2021-04-05 или 2021-03-05, вы можете столкнуться с проблемой, при которой приложение Kaspersky не может автоматически обнаруживать загруженное вредоносное ПО в веб-браузерах (подтверждено для Chrome и Mozilla). Мы рекомендуем вам запускать сканирование вручную каждый раз, когда вы загружаете что-либо в веб-

браузере, а также настоятельно рекомендуем вам не загружать неизвестные файлы в веб-браузерах.

- Могут возникнуть проблемы с активацией подписки, если время на вашем устройстве установлено с погрешностью более двух часов. Если при активации подписки вы столкнулись с проблемами, убедитесь, что на устройстве правильно выставлены дата и время. Если это не помогает, пожалуйста, обратитесь в службу технической поддержки.

- Если на устройстве включен режим энергосбережения, следующие функции приложения будут ограничены:

  - Устройства в моей сети

- На устройствах с Android 9-12.x 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 "Устройства в моей сети" 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.

  Как включить геолокацию на устройстве

  1. Откройте приложение **Настройки**.
  2. Нажмите **Местоположение**.

     Название раздела может отличаться в зависимости от модели устройства и версии Android (например, **Защита и местоположение**).

  3. Включите переключатель.

[Как предоставить приложению Kaspersky доступ к геолокации]

1. Откройте приложение **Настройки**.
2. Нажмите **Приложения**.

   В зависимости от модели и операционной системы устройства название раздела для управления приложениями может отличаться (например, **Диспетчер приложений**).

3. В списке приложений найдите приложение Kaspersky и нажмите на него.
4. В разделе **Разрешения** включите переключатель **Местоположение**.

- На устройствах с Android 4 для правильной работы приложения нужна последняя версия Google Play Services. В противном случае часть функций приложения Kaspersky может работать неправильно.
- На некоторых устройствах с Android 6.0-12.x функции "Интернет-защита" и "Защита чатов" могут не работать в режиме экономии заряда батареи. Сетевая активность блокируется для экономии заряда аккумулятора, поэтому приложение Kaspersky теряет соединение с Kaspersky Security Network. Это делает невозможной проверку безопасности ссылок. Чтобы возобновить использование Интернет-защиты, воспользуйтесь одним из следующих вариантов:

  1. Выключите режим экономии заряда батареи вручную или зарядите устройство до уровня, при котором режим экономии заряда батареи отключается автоматически.
  2. Добавьте приложение Kaspersky в список исключений для режима экономии заряда батареи.

- Приложение Kaspersky несовместимо с Xposed Framework.

  Для правильной работы приложения Kaspersky:

  1. Удалите Xposed Framework.
  2. Удалите приложение Kaspersky.
  3. Установите приложение Kaspersky.
  4. Активируйте приложение Kaspersky.

- Во время установки приложения Kaspersky вы можете столкнуться с ошибкой Error -24.

  Чтобы исправить эту ошибку:

  1. Если у вас есть права администратора на устройстве, вручную удалите папку: /data/data/com.kms.free.

  2. Если у вас нет прав администратора, перейдите в **Настройки** → **Приложения** . Очистите кеш и данные для Google Play Store и сервисов Google Play. Названия кнопок могут незначительно отличаться для разных версий Android.

  3. Попробуйте еще раз установить приложение Kaspersky.

  Если приведенные выше инструкции не помогли:

  1. Удалите аккаунт Google со своего устройства. См. инструкции в справке Google.

  2. Перезапустите устройство.

  3. Добавьте аккаунт Google на свое устройство. См. инструкции в справке Google.

  4. Попробуйте еще раз установить приложение Kaspersky.

  5. Если проблема не исправлена, попробуйте обновить операционную систему до Android 5.0–12.x.

Недоступность VPN в отдельных регионах

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

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

В перечисленных странах функция "Безопасное VPN-соединение" недоступна. "Лаборатория Касперского" старается максимально ограничить приобретение подписки на безопасное VPN-соединение в этих регионах.

Если вы ошибочно приобрели подписку на безопасное VPN-соединение в одном из перечисленных выше регионов, рекомендуется воспользоваться одним из следующих способов:

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

Устройства ASUS

В приложении Kaspersky могут быть следующие проблемы (и решения) на устройствах ASUS:

- На устройствах с установленным Asus Mobile Manager, если после настройки приложения Kaspersky вы закроете это приложение в списке запущенных, Asus Mobile Manager может заблокировать автозапуск приложения Kaspersky. В результате, приложение Kaspersky не сможет получать и выполнять команды от My Kaspersky.
- В связи с функциональностью прошивки, на устройствах ASUS ZenFone 2 после перезагрузки устройства может не начаться автозапуск приложения. Мы рекомендуем вам добавить приложение Kaspersky в список приложений, которые могут запускаться автоматически, или запускать приложение вручную после перезагрузки устройства.
- На устройствах Asus под управлением Android 7.1.1 команда **Удаление данных** может не удалить данные с SD-карты. Чтобы снизить риск попадания информации в чужие руки, на этих устройствах не храните конфиденциальную информацию на SD-картах.
- На устройстве Asus ZenFone 4 Max (ZC554KL) может не работать блокировка спам-звонков.
- Из-за определенных особенностей прошивки устройств ASUS могут возникнуть проблемы при вводе пароля с использованием любых раскладок, кроме английской. Переключение языка в поле ввода пароля не работает. Известно, что такая проблема возникает на ASUS ZenFone 6.

  Чтобы ввести пароль не на английском языке, используйте один из следующих вариантов:

  1. Установите стороннюю клавиатуру из Google Play и используйте ее для ввода пароля.
  2. Введите пароль в другом приложении, затем скопируйте и вставьте его в поле ввода пароля.

Устройства HTC

Приложение Kaspersky имеет следующие известные проблемы и возможные решения на устройствах HTC:

Из-за определенных особенностей прошивки устройств HTC могут возникнуть проблемы при вводе пароля с использованием любых раскладок, кроме английской.

Переключение языка в поле ввода пароля не работает. Известно, что эта проблема возникает на HTC M8.

Чтобы ввести пароль не на английском языке, используйте один из следующих вариантов:

1. Установите стороннюю клавиатуру из Google Play и используйте ее для ввода пароля.
2. Введите пароль в другом приложении, затем скопируйте и вставьте его в поле ввода пароля.

Устройства Huawei и Honor

На устройствах HUAWEI с оболочками EMUI требуется выполнить первоначальную настройку для правильной работы приложения Kaspersky.

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

Шаг 1. Исключите приложение Kaspersky из режима оптимизации батареи

Выполните этот шаг, чтобы разрешить отображение всплывающих окон для входящих звонков при включенном режиме энергосбережения.

Как исключить приложение из режима оптимизации работы батареи

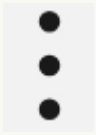
1. Откройте настройки устройства. Например, потяните строку состояния вниз и нажмите  .
2. Нажмите **Приложения**.

3. Выполните следующие действия:

   Для устройств с оболочкой EMUI 9.x:

   a. Нажмите **Приложения**.

      > Вы можете пропустить этот шаг на некоторых устройствах в зависимости от установленной прошивки.

   b. В правом верхнем углу нажмите  и в меню выберите **Специальный доступ**.

   c. Нажмите **Оптимизация батареи**.

   d. Найдите **приложение Kaspersky** и нажмите на него.

   e. Выберите **Запретить** для **приложения Kaspersky**, чтобы исключить приложение из режима экономии заряда батареи.

   Для устройств с оболочкой EMUI 8.x:

   a. В нижней части экрана нажмите  и выберите **Специальный доступ**.

   b. Нажмите **Игнорировать оптимизацию батареи**.

   c. Найдите **приложение Kaspersky** и нажмите на него.

   d. Выберите **Разрешить** для приложения Kaspersky, чтобы разрешить приложению игнорировать оптимизацию работы батареи.

Шаг 2. Закрепите приложение Kaspersky в оперативной памяти устройства

Выполните этот шаг, чтобы приложение не было выгружено из оперативной памяти устройства средствами операционной системы.

Как закрепить приложение в оперативной памяти устройства

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

1. Откройте список всех запущенных на устройстве приложений. Например, нажмите и удерживайте среднюю кнопку, пока на экране не появится список всех запущенных приложений.

2. Выполните одно из следующих действий:

   - Для устройств с оболочкой EMUI 9.x смахните **приложение Kaspersky** вниз.

     Появится значок  .

   - Для устройств с оболочкой EMUI 8.x выберите **приложение Kaspersky** и нажмите на  значок .

Значок  показывает, что приложение запущено.

Шаг 3. Включите ручное управление способом запуска приложения Kaspersky

Выполните этот шаг, чтобы вы могли управлять способом запуска приложения.

Как включить ручное управление способом запуска приложения

1. Откройте настройки устройства. Например, потяните строку состояния вниз и нажмите  .

2. Нажмите **Батарея**.

3. Нажмите **Запуск приложений**.

4. Найдите приложение **Kaspersky**и установите переключатель **Автоматическое управление** в состояние ВЫКЛ.

5. Убедитесь, что все переключатели **Управления вручную** (**Автозапуск**, **Косвенный запуск** и **Работа в фоновом режиме**) находятся в состоянии ВКЛ. Если необходимо, установите эти переключатели в состояние ВКЛ.

6. Нажмите **ОК**.

Приложение Kaspersky также имеет следующие известные проблемы и возможные решения на устройствах HUAWEI и HONOR:

- Из-за функциональности прошивки на Huawei P30 приложение может не запускаться автоматически после перезагрузки устройства. Мы рекомендуем вам добавить приложение Kaspersky в список приложений, которые могут запускаться автоматически, или запускать приложение вручную после перезагрузки устройства.

- На устройствах Huawei с операционной системой Android 6.0 и ниже, а также на устройствах Asus с операционной системой Android 7.1.1, команда **Удаление данных** может не удалить данные с SD-карты. Чтобы снизить риск попадания информации в чужие руки, на этих устройствах не храните конфиденциальную информацию на SD-картах.

- На некоторых устройствах Huawei возможность входа в My Kaspersky с помощью учетной записи Google может быть недоступна.

Устройства Lenovo

Приложение Kaspersky имеет следующие известные проблемы и возможные решения на устройствах Lenovo:

- На устройствах Lenovo с операционной системой Android 6.0 и ниже команда **Удаление данных** может не удалить данные с SD-карты. Чтобы снизить риск попадания информации в чужие руки, на этих устройствах не храните конфиденциальную информацию на SD-картах.

- Приложение может быть выгружено из оперативной памяти устройства средствами операционной системы. Если приложение выгружено, оно может не запускаться во время входящего телефонного звонка. Чтобы решить эту проблему, закрепите приложение в оперативной памяти устройства.

  Как закрепить приложение в оперативной памяти устройства

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

1. Откройте Менеджер задач. Например, нажмите и удерживайте правую кнопку, пока на экране не появится список всех запущенных приложений.
2. Выберите приложение Kaspersky.
3. Нажмите на значок замка рядом с названием приложения.

   Значок  показывает, что приложение запущено.

Устройства Meizu

Приложение Kaspersky имеет следующие известные проблемы и возможные решения на устройствах Meizu:

- Приложение Kaspersky может работать некорректно, если устройство находится в спящем режиме. Чтобы решить эту проблему, нажмите **Настройки** > **Устройство** > **Управление питанием** > **Энергосбережение** > **Оптимизация энергосбережения** > **Управление спящим режимом** и разрешите приложению Kaspersky продолжать работу в спящем режиме.

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

- Приложение Kaspersky может не запускаться после перезагрузки устройства или выгрузки из оперативной памяти. Чтобы решить эту проблему, разрешите автоматический перезапуск для приложения Kaspersky.

- Приложение Kaspersky может выгружаться из оперативной памяти устройства. Для правильной работы приложения вам нужно закрепить приложение в оперативной памяти.

  Как закрепить приложение в оперативной памяти устройства

  Например: на Meizu M5 Note Flyme 6 нажмите **Безопасность** > **Разрешения** > **Запуск в фоне** > приложение Kaspersky > **Разрешить работу в фоне**.

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

- MEIZU M2 MINI:

  Всплывающее окно с определителем номера может не отображаться на устройствах Meizu M2 mini с системой Flyme 5.

- MEIZU PRO 6 PLUS:

  Приложение Kaspersky может не получить доступ к разрешениям на устройстве Meizu Pro 6 Plus с Android 6.0.1, поэтому может работать неправильно. Чтобы решить эту проблему, обновите операционную систему Android до версии 7.x. Если вы не можете обновить операционную систему, выполните следующие действия:

  1. Нажмите **Настройки** > **Приложения** > **Kaspersky** > **Управление разрешениями**.
  2. Выдайте приложению все разрешения. Для этого установите переключатели разрешений в состояние ВКЛ или нажмите на разрешение и выберите **Разрешить**.

- На устройствах Meizu секретный код функции "Где мое устройство" не должен содержать более 4 цифр.

  Если вы установите секретный код, содержащий более 4 цифр, вы не сможете разблокировать устройство с его помощью. В этом случае вам придется обратиться в сервисный центр Meizu для восстановления доступа к устройству.

- После того, как вы отправите команду "Сделать тайное фото" через функцию Где мое устройство на устройстве Meizu, устройство может отобразить запрос на доступ к камере или службе определения местоположения вместо того, чтобы заблокировать устройство. Известно, что такая проблема возникает на Meizu MX4.

Устройства Nubia

Приложение Kaspersky имеет следующие известные проблемы и возможные решения на устройствах Nubia:

- В связи с функциональностью прошивки, на устройствах Nubia NX 529 после перезагрузки устройства может не начаться автозапуск приложения. Мы рекомендуем вам добавить приложение Kaspersky в список приложений, которые могут запускаться автоматически, или запускать приложение вручную после перезагрузки устройства.

Устройства SAMSUNG

Следующие устройства SAMSUNG не поддерживаются:

- Samsung GT-I9300i Galaxy S3 Duos
- Samsung GT-I9301i Galaxy S3 Neo

Установка приложения на эти устройства может вызвать ошибки и потерю данных.

Приложение Kaspersky нельзя установить на эти устройства через Google Play.

Если вы уже приобрели подписку на приложение Kaspersky, запросите возврат средств в технической поддержке "Лаборатории Касперского" через My Kaspersky.

Приложение Kaspersky имеет следующие известные проблемы и возможные решения на устройствах SAMSUNG:

- В связи с функциональностью прошивки, на устройствах Samsung Galaxy A9 после перезагрузки устройства может не начаться автозапуск приложения. Мы рекомендуем вам добавить приложение Kaspersky в список приложений, которые могут запускаться автоматически, или запускать приложение вручную после перезагрузки устройства.
- На устройствах с операционной системой Android 6 и Samsung S7 с операционной системой Android 7 с прошивкой ниже, чем G930FXXU1DQD7 / G930FOZS1DQD8 / G930FXXU1DQC8, если вы копируете вредоносное ПО в диспетчере файлов, Автоматический Антивирус не обнаруживает его. Это происходит из-за известной проблемы Android 6 и проблемы устройств Samsung (P170213-05125). По этой причине приложение не может отслеживать изменения в файловой системе устройства. Если вы запустите проверку устройства, приложение найдет это вредоносное ПО. Рекомендуем обновить прошивку или регулярно запускать проверку устройства.
- На устройствах Samsung с операционной системой Android 9, если приложение заблокировано функцией Блокировка приложений, его можно разблокировать только с помощью графического ключа или секретного кода. Разблокировка по отпечатку пальца недоступна.
- Приложение Kaspersky может не запускаться после перезагрузки устройства. Чтобы решить эту проблему, разрешите автоматический перезапуск для приложения Kaspersky. Например, используйте приложение **Smart Manager**. Для этого нажмите **Smart Manager >ОЗУ > Прил.Автозагр.** и включите переключатель приложения Kaspersky.

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

- Из-за некоторых особенностей прошивки устройств Samsung могут возникнуть проблемы при вводе пароля с использованием любых раскладок, кроме английской. Если приложениям предоставлены специальные разрешения, раскладка клавиатуры может быть недоступна. Известно, что такая проблема возникает на Samsung Galaxy S4.

  Чтобы ввести пароль не на английском языке, используйте один из следующих вариантов:

  - Установите стороннюю клавиатуру из Google Play и используйте ее для ввода пароля.
  - Отключите специальные разрешения для приложений и попробуйте ввести пароль еще раз. Отключение специальных разрешений может повлиять на работу приложений.

- На устройствах с оболочкой One UI 2.1 и выше, если приложение Kaspersky помещено (пользователем или автоматически устройством) в список приложений, находящихся в режиме глубокого сна, основная функциональность приложения может быть потеряна. Для правильной работы добавьте приложение Kaspersky в список никогда не спящих приложений.

  Как добавить приложение в список никогда не спящих приложений

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

  1. Перейдите в **Настройки** вашего устройства.
  2. Нажмите **Аккумулятор и уход за устройством** > **Аккумулятор** > **Ограничения фонового использования** .
  3. В открывшемся окне добавьте приложение Kaspersky в список **Никогда не спящие приложения**.

Устройства XIAOMI

На устройствах XIAOMI требуется начальная настройка, чтобы обеспечить правильную работу приложения Kaspersky.

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

Шаг 1. Выдайте приложению Kaspersky специальные разрешения

Выполните этот шаг, чтобы разрешить приложению правильно выполнять следующие функции:

- отображать всплывающее окно с определителем номера для входящих звонков, когда устройство заблокировано;
- отображать всплывающее окно, когда приложение работает в фоновом режиме;
- обеспечить правильную работу со всплывающими окнами, когда приложение работает в фоновом режиме.

Как вручную предоставить приложению специальные разрешения

1. Откройте приложение **Настройки**.
2. Выполните одно из следующих действий:
   - Нажмите **Приложения** > **Разрешения** > **Другие разрешения**.
   - Нажмите **Разрешения**> **Другие разрешения**.

   Расположение раздела **Разрешения** в настройках устройства может отличаться в зависимости от установленной прошивки.
3. Выберите приложение **Kaspersky**.
4. В разделе **Настройки** нажмите на название разрешения и выберите **Разрешить**, чтобы предоставить приложению следующие разрешения:
   - **Экран Блокировки**. Это разрешение позволяет отображать всплывающее окно с определителем номера для входящих звонков, когда устройство заблокировано.
   - **Запуск в фоне** или **Отображать всплывающие окна, когда запущено в фоновом режиме**. Это разрешение позволяет отображать всплывающее окно, когда приложение работает в фоновом режиме.

- **Всплывающие окна**. Это разрешение позволяет обеспечить правильную работу со всплывающими окнами, когда приложение работает в фоновом режиме.

Шаг 2. Закрепите приложение Kaspersky в оперативной памяти устройства

Выполните этот шаг, чтобы приложение не было выгружено из оперативной памяти устройства средствами операционной системы.

Как закрепить приложение в оперативной памяти устройства

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

1. Откройте список всех запущенных на устройстве приложений. Например, нажмите и удерживайте среднюю кнопку, пока на экране не появится список всех запущенных приложений.
2. Выполните одно из следующих действий:

   - Смахните **Приложение Kaspersky** вниз. Появится значок  .
   - Выберите приложение **Kaspersky** и нажмите на значок  .

   Значок  показывает, что приложение запущено.

Приложение Kaspersky также имеет следующие известные проблемы и возможные решения на устройствах XIAOMI:

- Приложение может перестать работать, находясь в фоновом режиме, даже если оно было закреплено в оперативной памяти. Чтобы решить эту проблему, поменяйте настройку для контроля активности приложения в настройках батареи.

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

Например, на устройстве Xiaomi Redmi Note 3 с Android 6.0.1 нажмите **Настройки** > **Батарея и производительность** > **Расход заряда батареи приложениями** > **Выбрать приложения** (доступно при включенном энергосбережении) > **Kaspersky** > **Нет ограничения**.

- Приложение Kaspersky может не запускаться после перезагрузки устройства или выгрузки из оперативной памяти. Чтобы решить эту проблему, разрешите автоматический перезапуск для приложения Kaspersky в Центре безопасности на устройстве.

- В связи с функциональностью прошивки, на устройствах Xiaomi Redmi Note 3 после перезагрузки устройства может не начаться автозапуск приложения. Мы рекомендуем вам добавить приложение Kaspersky в список приложений, которые могут запускаться автоматически, или запускать приложение вручную после перезагрузки устройства.

- "Интернет-защита" может работать неправильно на устройствах Xiaomi: фильтрация вредоносных и фишинговых веб-сайтов может не работать. Используйте один из следующих способов, чтобы обеспечить полноценную защиту вашего устройства:

  a. Используйте браузер Chrome, который поддерживает Интернет-защиту.

  b. В приложении Kaspersky для Android перейдите в настройки Интернет-защиты и нажмите **Разрешить доступ**. Следуйте инструкциям на экране вашего устройства и предоставьте приложению необходимые разрешения.

- После того, как вы отправите команду "Сделать тайное фото" через функцию Где мое устройство на устройстве Xiaomi, устройство может отобразить запрос на доступ к камере или службе определения местоположения вместо того, чтобы заблокировать устройство. Известно, что такая проблема возникает на Xiaomi Redmi Note 3.

Устройства ZTE

Приложение Kaspersky имеет следующие известные проблемы и возможные решения на устройствах ZTE:

- Приложение может не запуститься автоматически после перезапуска устройства или выгрузки приложения из памяти устройства. В этом случае вы должны запустить приложение вручную.

- Приложение может быть выгружено из оперативной памяти устройства средствами операционной системы. Чтобы решить эту проблему, закрепите приложение в оперативной памяти устройства.

  Как закрепить приложение в оперативной памяти устройства

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

1. Откройте Менеджер задач. Например, удерживайте среднюю кнопку, пока не появится список всех запущенных приложений.
2. Выберите приложение Kaspersky.
3. Нажмите на значок  рядом с названием приложения.

   Значок  показывает, что приложение запущено.

- Приложение может перестать работать, находясь в фоновом режиме, даже если оно было закреплено в оперативной памяти. Чтобы решить эту проблему, измените настройки контроля приложения в настройках батареи.

  Например, на ZTE Blade V7 с Android 6.0 нажмите **Настройки** > **Батарея** > **Экономия заряда батареи** > **Все приложения** > **Kaspersky** > **Не экономить**.

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

- Уведомления от приложения Kaspersky могут не отображаться или отображаются неправильно. Чтобы решить эту проблему, на ZTE blade v7 с Android 6.0 нажмите **Настройки** > **Приложения** > **Kaspersky** > **Уведомления** > **Считать важным**.

Правовая информация

Просмотр условий лицензионного соглашения и других юридических документов

Чтобы просмотреть юридический документ:

1. В главном окне приложения нажмите ☰ или смахните вправо.

   Слева появится панель быстрого доступа.

2. В боковом меню нажмите **О приложении** > Правовая 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, 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.

Бета-тестирование

О бета-версии

Бета-версии недоступны для использования на территории США. 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. В бета-версии приложений вы сможете воспользоваться новыми функциями, которые еще не представлены официально.

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

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

Вы должны использовать приложение только в соответствии с функциональностью, предоставляемой установленной версией приложения. Чтобы просмотреть список приложений, бета-версии которых вы используете, перейдите в Google Play и нажмите **Профиль** > **Мои приложения и игры** > **Бета-версии**.

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

Поучаствовать в бета-тестировании

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

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

Отправка отзыва

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

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

Если вы уже приобрели лицензию, 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 My Kaspersky, в справке My Kaspersky .

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