kaspersky

Kaspersky Internet Security для Android

Руководство по эксплуатации

Версия программы: 11.69.4.5763

Содержание

О Kaspersky Internet Security для Android

Kaspersky Internet Security для Android обеспечивает комплексную защиту ваших мобильных устройств. В составе Kaspersky Internet Security для Android предусмотрены следующие функции и компоненты защиты:

Функции и компоненты Kaspersky Internet Security для Android

Функции	Компоненты	
	Бесплатная версия	Премиум-версия
Защита от вирусов и других вредоносных приложений	Сканер	Постоянная защита
Защита от интернет-угроз	Недоступно	Интернет-защита
	Недоступно	Защита чатов
Защита данных при потере или краже устройства	Анти-Вор	Анти-Вор
Защита доступа к приложениям с помощью секретного кода	Недоступно	Блокировка приложений
Блокировка нежелательных звонков	Фильтр звонков	Фильтр звонков
Оптимизация пространства устройства и проверка выданных разрешений	Мои приложения	Мои приложения

Сканер

Вы можете запускать следующие виды проверки:

- Полная проверка

  Kaspersky Internet Security 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.

- Быстрая проверка

  Kaspersky Internet Security проверяет только установленные приложения.

- 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.

Постоянная защита

Постоянная защита 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.

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.

Защита чатов

Функция Защита чатов проверяет SMS-сообщения и сообщения, которые вы получаете через WhatsApp, Viber, Telegram и Google Hangouts, на наличие фишинговых ссылок.

Анти-Вор

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

Блокировка приложений

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

Фильтр 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.

Мои приложения

Компонент Мои приложения позволяет оптимизировать пространство устройства и проверить, какие разрешения вы выдали приложениям, установленным на устройстве. Узнайте, какие приложения вы не используете, и удалите их. Узнайте о возможных рисках выданных разрешений.

Часто задаваемые вопросы

Активация премиум-версии приложения

Чтобы использовать все функции приложения, вам нужно активировать премиум-версию Kaspersky Internet Security. Чтобы активировать премиум-версию, вы должны приобрести подписку.

Для активации премиум-версии приложения нужно интернет-соединение.

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

- Использовать подписку, найденную в вашей учетной записи 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 премиум-версию при первом запуске приложения или в любое время позже.

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

Покупка подписки через Google Play

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

1. Откройте Kaspersky Internet Security.
2. Нажмите на  .
3. В верхней части меню нажмите на иконку  с информацией о подписке.
4. Нажмите **Активировать премиум-версию**.

   Если для вашей учетной записи My Kaspersky обнаружена подписка, по которой можно активировать приложение, Kaspersky Internet Security предложит вам использовать ее для активации. Если вы выберете эту подписку, приложение автоматически активирует премиум-версию. Если подписка не найдена или вы предпочитаете приобрести подписку в Google Play, выберите план подписки, который вы хотите приобрести.
5. Нажмите **ПОДПИСАТЬСЯ**.
6. Завершите покупку в Google Play.

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

Активация премиум-версии по подписке, найденной в вашей учетной записи My Kaspersky

1. Откройте Kaspersky Internet Security.

2. Нажмите на  .
3. Убедитесь, что вы вошли в вашу учетную запись My Kaspersky. В противном случае нажмите **Войти в My Kaspersky**.
4. В верхней части меню нажмите на иконку  с информацией о подписке.
5. Нажмите **Активировать премиум-версию**.

   Если для вашей учетной записи My Kaspersky обнаружена подписка, по которой можно активировать приложение, Kaspersky Internet Security 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 премиум-версии приложения с помощью кода активации

1. Откройте Kaspersky Internet Security.
2. Нажмите на  .
3. В верхней части меню нажмите на иконку  с информацией о подписке.
4. Нажмите **Активировать премиум-версию**.
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 премиум-версии приложения. Например, пользователи предустановленной версии Kaspersky Internet Security на устройствах Samsung в России также могут управлять своими подписками через учетную запись Softline.

Когда до окончания срока действия подписки остается менее 14 дней, вы можете продлить его. При использовании приложения по подписке вы не можете применить другой код активации для продления срока действия подписки. Это будет возможно после окончания подписки или после отказа от подписки.

На устройствах Huawei без сервисов Google Play вы можете активировать премиум-версию Kaspersky Internet Security , войдя в свою учетную запись My Kaspersky или используя код активации.

На устройствах Samsung с предустановленным приложением Kaspersky Internet Security вы можете приобрести подписку, продлевать ее и управлять ею через свою учетную запись Softline.

Обновление антивирусных баз

При поиске вредоносных приложений Kaspersky Internet Security использует антивирусные базы. Антивирусные базы приложения содержат описание вредоносных 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 Kaspersky Internet Security нажмите **Обновление**.

В премиум-версии Kaspersky Internet Security вы можете настроить расписание автообновлений антивирусных баз.

Как запланировать автообновление

1. В главном окне Kaspersky Internet Security для Android нажмите **Постоянная защита** .
2. Выберите **Обновление** .
3. Нажмите **Расписание** 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.

О проверке

Вы можете запускать следующие виды проверки:

- Полная проверка

  Kaspersky Internet Security 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 Kaspersky Internet Security 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. В премиум-версии расширенная версия этой проверки доступна как часть Постоянной защиты .

- Проверка всех файлов по расписанию. В премиум-версии вы можете настроить расписание, согласно которому приложение будет проверять все файлы на вашем устройстве.

- Быстрая проверка

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

  Если вы не хотите запускать проверку вручную, в премиум-версии можно 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.

Об Анти-Воре

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

По умолчанию функция Анти-Вор выключена. Чтобы удаленно отправлять команды на ваше устройство, включите на устройстве функцию Анти-Вор. Потренируйтесь использовать отдельные функции прямо сейчас, чтобы в случае кражи или потери устройства вы смогли действовать без замешательства.

Если вы не включили функцию Анти-Вор 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:

- заблокировать устройство и определить его местоположение;
- 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 Анти-Вор 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 Kaspersky Internet Security и защиту от изменения системных настроек.

Настройки Анти-Вора защищены блокировкой экрана.

О Блокировке приложений

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

Блокировка приложений доступна только в премиум-версии Kaspersky Internet Security.

Kaspersky Internet Security 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 Kaspersky Internet Security, установив флажок **Защита от удаления** в настройках Анти-Вора.

Подписка и учетная запись

О бесплатной, пробной и премиум версиях

- *Бесплатная версия.* Бесплатная версия позволяет использовать ограниченную функциональность в течение неограниченного периода времени. С бесплатной версии вы можете перейти на пробную версию или премиум-версию приложения.

  Бесплатная версия доступна сразу после установки приложения.

- *Пробная версия.* При покупке автоматически продлеваемой подписки вы получаете ознакомительный период, в течение которого вы можете бесплатно пользоваться функциями приложения премиум-версии Kaspersky Internet Security. Пробный период дается один раз. По истечении пробного периода ваш поставщик услуг автоматически спишет с вас оплату за подписку.

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

- *Премиум-версия.* Премиум-версия предоставляет доступ ко всем функциям приложения. Премиум-версия доступна после покупки подписки на приложение. По истечении срока действия подписки приложение автоматически переходит на бесплатную версию. Чтобы продолжить использование приложения, продлите подписку или переключитесь на бесплатную версию приложения.

О подписке на Kaspersky Internet Security

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 свою учетную запись. Способы управления подпиской зависят от вашего провайдера. Например, по ссылкам приведены инструкции для Google Play и Huawei.

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 Kaspersky Internet Security будут применены ограничения бесплатной версии приложения.

Чтобы использовать Kaspersky Internet Security по подписке, вам необходимо войти в My Kaspersky в приложении Kaspersky Internet Security и активировать премиум-версию .

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

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.

Оформление подписки на Kaspersky Internet Security для Android не отменяет других ваших подписок, распространяющихся на Kaspersky Internet Security для Android. Чтобы избежать дополнительных платежей, убедитесь в том, что вы отменили или отключили автопродление подписки, которая вам не нужна.

Отмена подписки на Kaspersky Internet Security для Android или переход на продление подписки вручную:

1. Перейдите на страницу вашей учетной записи на сайте поставщика услуг.
2. Проверьте активные подписки, которые могут распространяться на Kaspersky Internet Security для Android.
3. Отмените или отключите автопродление подписок, которые вам не нужны.

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 премиум-версию приложения.

Чтобы проверить срок действия подписки и просмотреть подробную информацию:

1. Откройте Kaspersky Internet Security.
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 премиум-версии приложения

Чтобы использовать все функции приложения, вам нужно активировать премиум-версию Kaspersky Internet Security. Чтобы активировать премиум-версию, вы должны приобрести подписку.

Для активации премиум-версии приложения нужно интернет-соединение.

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

- Использовать подписку, найденную в вашей учетной записи 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 премиум-версию при первом запуске приложения или в любое время позже.

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

Покупка подписки через Google Play

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

1. Откройте Kaspersky Internet Security.
2. Нажмите на  .
3. В верхней части меню нажмите на иконку  с информацией о подписке.
4. Нажмите **Активировать премиум-версию**.

   Если для вашей учетной записи My Kaspersky обнаружена подписка, по которой можно активировать приложение, Kaspersky Internet Security предложит вам использовать ее для активации. Если вы выберете эту подписку, приложение автоматически активирует премиум-версию. Если подписка не найдена или вы предпочитаете приобрести подписку в Google Play, выберите план подписки, который вы хотите приобрести.
5. Нажмите **ПОДПИСАТЬСЯ**.
6. Завершите покупку в Google Play.

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

Активация премиум-версии по подписке, найденной в вашей учетной записи My Kaspersky

1. Откройте Kaspersky Internet Security.
2. Нажмите на  .
3. Убедитесь, что вы вошли в вашу учетную запись My Kaspersky. В противном случае нажмите **Войти в My Kaspersky**.
4. В верхней части меню нажмите на иконку  с информацией о подписке.
5. Нажмите **Активировать премиум-версию**.

   Если для вашей учетной записи My Kaspersky обнаружена подписка, по которой можно активировать приложение, Kaspersky Internet Security 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 премиум-версии приложения с помощью кода активации]

1. Откройте Kaspersky Internet Security.
2. Нажмите на  .
3. В верхней части меню нажмите на иконку  с информацией о подписке.
4. Нажмите **Активировать премиум-версию**.
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 премиум-версии приложения. Например, пользователи предустановленной версии Kaspersky Internet Security на устройствах Samsung в России также могут управлять своими подписками через учетную запись Softline.

Когда до окончания срока действия подписки остается менее 14 дней, вы можете продлить его. При использовании приложения по подписке вы не можете применить другой код активации для продления срока действия подписки. Это будет возможно после окончания подписки или после отказа от подписки.

На устройствах Huawei без сервисов Google Play вы можете активировать премиум-версию Kaspersky Internet Security , войдя в свою учетную запись My Kaspersky или используя код активации.

На устройствах Samsung с предустановленным приложением Kaspersky Internet Security вы можете приобрести подписку, продлевать ее и управлять ею через свою учетную запись Softline.

Предоставление данных

Об использовании приложения на территории Европейского союза

При распространении на территории Европейского союза, Kaspersky Internet Security 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 Kaspersky Internet Security на территории Европейского союза. После установки приложение предложит вам прочитать и принять условия, необходимые для первоначальной настройки и использования Kaspersky Internet Security.

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**.

   Отобразится текст соглашения, которое вы выбрали.
3. Прочитайте текст соглашения:
   - Если вы согласны предоставлять данные для этих целей, нажмите **Включить** и примите условия соглашения.
   - Если вы хотите отклонить соглашение, нажмите **Выключить**.

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.

- Kaspersky Internet Security 11.54.X.XXX
- Kaspersky Internet Security 11.41.4.XXXX
- Kaspersky Internet Security 11.34.4.2569
- Kaspersky Internet Security 11.27.4.2246
- Kaspersky Internet Security 11.23.4.2043
- Kaspersky Internet Security 11.20.4.1026

- Kaspersky Internet Security 11.20.4.806

Данные, передаваемые в "Лабораторию Касперского" приложением Kaspersky Internet Security, начиная с версии 1.44.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;

- название 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.

О предоставлении данных (другие регионы)

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

- Kaspersky Internet Security 11.54.X.XXX
- Kaspersky Internet Security 11.41.4.XXXX
- Kaspersky Internet Security 11.34.4.2569
- Kaspersky Internet Security 11.27.4.2246
- Kaspersky Internet Security 11.23.4.2043
- Kaspersky Internet Security 11.20.4.1026
- Kaspersky Internet Security 11.20.4.806

Данные, передаваемые в "Лабораторию Касперского" приложением Kaspersky Internet Security, начиная с версии 11.64.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** > **Правовая информация**.
2. Нажмите на название положения.

   Откроется содержание выбранного положения.

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

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

Установка и удаление приложения

Аппаратные и программные требования

Эта справка применима для Kaspersky Internet Security для Android версии 11.65.X.XXXX и более поздних.

Для функционирования Kaspersky Internet Security 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 4.4–11.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 atomx86 или ARMv7 и более поздние версии.

Приложение должно быть установлено в основную память устройства.

В случае использования часов для функционирования Kaspersky Internet Security устройство должно удовлетворять следующим требованиям:

- операционная система: Android 4.4–11.x
- поддержка Bluetooth на устройстве и часах;
- Kaspersky Internet Security, начиная с версии 11.10;
- часы Android Wear.

  Более подробная информация о часах Android Wear и устройствах приведена на сайте технической поддержки Android Wear.

Использование приложения на часах недоступно для устройств Huawei.

Установка приложения

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

Чтобы установить Kaspersky Internet Security, выполните следующие действия:

1. Откройте сайт или магазин приложений на вашем устройстве.
2. Выберите приложение Kaspersky Internet Security.
3. Откройте страницу приложения.

4. Ознакомьтесь со списком прав, которые нужны приложению Kaspersky Internet Security:

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

     Начнется установка приложения.

   - Если вы отказываетесь предоставить приложению необходимые разрешения, не устанавливайте 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 Kaspersky Internet Security для удаления приложения.

Чтобы удалить Kaspersky Internet Security с устройства, выполните следующие действия:

1. Откройте Kaspersky Internet Security.
2. Нажмите > **Настройки** > **Удалить приложение**.
3. В окне **Удаление Kaspersky Internet Security** нажмите **Далее**.
4. Если нужно, введите секретный код приложения.

   Приложение запрашивает секретный код, если в настройках Анти-Вора установлен флажок **Защита от удаления**.
5. Подтвердите удаление Kaspersky Internet Security.

Приложение Kaspersky Internet Security будет удалено с устройства.

Если вы включили Анти-Вор, Kaspersky Internet Security для Android назначен администратором устройства. Перед удалением Kaspersky Internet Security для Android 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 Kaspersky Internet Security.
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 Kaspersky Internet Security, вы можете отключить приложение в системных настройках устройства. Kaspersky Internet Security по-прежнему будет установлен 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 Kaspersky Internet Security 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 Kaspersky Internet Security нажмите **Проверка** > **Быстрая проверка**.

О проверке

Вы можете запускать следующие виды проверки:

- Полная проверка

  Kaspersky Internet Security 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 Kaspersky Internet Security 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. В премиум-версии расширенная версия этой проверки доступна как часть Постоянной защиты .

  - Проверка всех файлов по расписанию. В премиум-версии вы можете настроить расписание, согласно которому приложение будет проверять все файлы на вашем устройстве.

- Быстрая проверка

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

  Если вы не хотите запускать проверку вручную, в премиум-версии можно 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 Kaspersky Internet Security 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 Kaspersky Internet Security нажмите **Постоянная защита** > **Ручная и регулярная проверки**.
2. Выберите **Тип проверяемых файлов**.
3. 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.
4. Настройте частоту проверки, выбрав для параметра **По расписанию** значение **Раз в неделю**, **Раз в день** или **После обновления**.
5. 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 Kaspersky Internet Security 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 приложений Kaspersky Internet Security использует антивирусные базы. Антивирусные базы приложения содержат описание вредоносных 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 Kaspersky Internet Security нажмите **Обновление**.

В премиум-версии Kaspersky Internet Security вы можете настроить расписание автообновлений антивирусных баз.

Как запланировать автообновление

1. В главном окне Kaspersky Internet Security для Android нажмите **Постоянная защита** .
2. Выберите **Обновление** .
3. Нажмите **Расписание** 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.

Постоянная защита

Постоянная защита 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, в премиум-версии – Постоянная защита.

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 (Kaspersky Internet Security 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 **Постоянная защита** > **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.

Постоянная защита

Постоянная защита включает все функции Сканера и предоставляет автоматическую защиту устройства 24/7. Постоянная защита 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, Kaspersky Internet Security может классифицировать такую программу как вредоносную.

Настройка параметров Постоянной защиты

1. В панели быстрого запуска Kaspersky Internet Security нажмите **Постоянная защита**.
2. Нажмите **Постоянная защита** и выберите режим защиты: **Рекомендуемый** или **Расширенный**.

   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.

4. Если вы выбрали **Расширенный** режим защиты, настройте его параметры в разделе **Настройки** > **Постоянная защита**.

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

5. Выберите типы файлов для проверки в реальном времени: нажмите **Определенный файл или папку** и выберите значение.

6. Выберите действие приложения при обнаружении объекта во время проверки: нажмите **Действие при обнаружении** и укажите значение.

Анти-Вор

Об Анти-Воре

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

По умолчанию функция Анти-Вор выключена. Чтобы удаленно отправлять команды на ваше устройство, включите на устройстве функцию Анти-Вор. Потренируйтесь использовать отдельные функции прямо сейчас, чтобы в случае кражи или потери устройства вы смогли действовать без замешательства.

Если вы не включили функцию Анти-Вор 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:

- заблокировать устройство и определить его местоположение;
- 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 Анти-Вор 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 Kaspersky Internet Security и защиту от изменения системных настроек.

Настройки Анти-Вора защищены блокировкой экрана.

Включение функции Анти-Вор

Чтобы начать пользоваться функцией Анти-Вор, выполните следующие действия:

1. В панели быстрого запуска Kaspersky Internet Security нажмите **Анти-Вор**.

   Откроются настройки Анти-Вора.

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 вашу учетную запись My Kaspersky, если вы не сделали этого ранее.

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

7. Предоставьте приложению расширенные права путем активации Администратора устройства. Эти разрешения необходимы для выполнения команд Анти-Вора 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.

Анти-Вор настроен. Основные функции Анти-Вора включены. При необходимости включите дополнительные функции защиты: SIM-Контроль и защиту от удаления.

Если вы не хотите использовать отдельные функции компонента Анти-Вор, на главном экране Анти-Вора нажмите на панель с названием функции и выключите ее с помощью переключателя.

Контроль устройства через My Kaspersky

Если ваше устройство утеряно, можно отправлять команды компонента Анти-Вор удаленно через My Kaspersky.

Если на вашем устройстве настроена двухфакторная аутентификация для доступа к My Kaspersky с помощью кода SMS, вы не сможете войти в свою учетную запись и использовать функцию Анти-Вор в случае утери SIM-карты. Чтобы этого избежать, настройте аутентификацию на нескольких устройствах .

Чтобы отправить команды на утерянное устройство, выполните следующие действия:

1. Откройте My Kaspersky на любом устройстве.

2. Войдите на My Kaspersky с учетной записью, которая использовалась для настройки функции.

3. В разделе **Устройства** найдите требуемое устройство и нажмите на кнопку **Управлять**.
4. Перейдите на закладку **Команды**.
5. Нажмите на кнопку с названием команды, чтобы отправить ее на устройство.
6. Следуйте инструкциям для команды.

   Статус исполнения команды отобразится в окне команды.

Пример использования

Если вы потеряли ваше устройство где-то неподалеку, можно включить на устройстве сирену. Громкий звук поможет вам найти устройство. Следуйте приведенным в этом разделе инструкциям, чтобы отправить команду **Сирена** с помощью My Kaspersky.

Можно добавить сообщение, отображаемое на экране вашего устройства при срабатывании сирены. Например, можно добавить дополнительный номер телефона, чтобы человек, нашедший ваше устройство, мог связаться с вами.

После подтверждения включения сирены на My Kaspersky, ваше устройство будет заблокировано, сирена сработает и ваше сообщение появится на экране. Когда вы найдете ваше устройство, разблокируйте его с помощью вашего секретного кода, графического ключа или отпечатка пальца.

Настройка SIM-Контроль

Чтобы настроить параметры функции SIM-Контроль:

1. В панели быстрого запуска Kaspersky Internet Security нажмите **Анти-Вор**.
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.
5. Выберите поле **Текст при блокировании** и введите сообщение, которое будет отображаться на экране заблокированного устройства. Нажмите **Сохранить**.

Защита от удаления приложения

Вы можете защитить Kaspersky Internet Security от несанкционированного удаления с устройства. Если ваше устройство было украдено, злоумышленники не смогут удалить Kaspersky Internet Security и помешать вам воспользоваться функцией Анти-Вор.

Изменение отдельных системных параметров нарушает работу функций защиты в Kaspersky Internet Security. 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 Kaspersky Internet Security от несанкционированного удаления:

1. В панели быстрого запуска Kaspersky Internet Security нажмите **Анти-Вор**.
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.

Kaspersky Internet Security будет запрашивать секретный код при попытке удалении приложения 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.

Блокировка приложений

О Блокировке приложений

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

Блокировка приложений доступна только в премиум-версии Kaspersky Internet Security.

Kaspersky Internet Security 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 Kaspersky Internet Security, установив флажок **Защита от удаления** в настройках Анти-Вора.

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 Kaspersky Internet Security.
2. Нажмите **Блокировка приложений**.

Запустится мастер первоначальной настройки Блокировки приложений.

3. Просмотрите описание функции и нажмите **Далее**.
4. Включите специальные возможности для Kaspersky Internet Security. 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 Kaspersky Internet Security.

   c. Включите переключатель для Kaspersky Internet Security.

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

   e. Возвратитесь в Kaspersky Internet Security.
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 Анти-Вора 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 Kaspersky Internet Security.
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 Kaspersky Internet Security.
2. Разблокируйте доступ к приложению с помощью секретного кода, графического ключа или отпечатка пальца.

   Приложение откроется.

Интернет-защита

Об Интернет-защите

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 в премиум-версии Kaspersky Internet Security.

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 Kaspersky Internet Security.
2. Нажмите **Интернет-защита**.

   Запустится мастер первоначальной настройки.
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 Kaspersky Internet Security.
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 Kaspersky Internet Security, 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 в премиум-версии Kaspersky Internet Security.

Веб-контроль позволяет управлять веб-контентом на мобильном устройстве и защищать от нежелательного онлайн-контента. Например, вы можете установить Kaspersky Internet Security на устройство вашего ребенка и выбрать, какие категории веб-материалов и конкретные веб-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 Kaspersky Internet Security.
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 **Защищенный браузер**.

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 в премиум-версии Kaspersky Internet Security.

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

На устройствах с Android 4.4 ограниченная функциональность Защиты чатов доступна как SMS Анти-Фишинг .

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 Kaspersky Internet Security в панели быстрого запуска нажмите **Защита чатов**.
2. Нажмите **Проверка ссылок в SMS**.
3. Установите переключатель **Предупреждать об опасных ссылках** в положение ВКЛ.

   Kaspersky Internet Security 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 Kaspersky Internet Security в панели быстрого запуска нажмите **Защита чатов**.
2. Нажмите **Проверка ссылок в мессенджерах**
3. Установите переключатель **Блокировать опасные ссылки** в положение ВКЛ.

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

SMS Анти-Фишинг (для устройств с Android 4.4 и 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 с Android 4.4 и для устройств Huawei без браузера Google Chrome. На устройствах с браузером Google Chrome и Android 4.5 и более поздних доступна расширенная версия этой функции (см. Защита чатов).

SMS Анти-Фишинг доступен только в премиум-версии Kaspersky Internet Security.

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

Чтобы проверять ссылки в SMS-сообщениях:

1. В главном окне Kaspersky Internet Security 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 и более поздними версиями, 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 Kaspersky Internet Security 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 **Подсказка после звонка** включена, приложение предложит вам заблокировать этот номер после звонка.

В окне подсказки выберите одно из следующих действий:

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

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

Все звонки с этого номера будут заблокированы.

Как отредактировать контакт в списке запрещенных номеров?

1. В панели быстрого запуска Kaspersky Internet Security 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 Kaspersky Internet Security 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 Kaspersky Internet Security 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 **Подсказка после звонка** недоступна на устройствах с операционной системой Android 9 и выше.

Чтобы включить подсказку:

1. В панели быстрого запуска Kaspersky Internet Security нажмите **Фильтр звонков**.
2. Включите переключатель **Подсказка после звонка**.

Теперь после завершения или отклонения звонка вы будете видеть подсказку.

> Если на вашем устройстве установлено приложение Kaspersky Who Calls, Kaspersky Internet Security 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 компоненте Мои приложения

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

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

В разделе **Приложения** экрана Мои приложения вы можете просмотреть список приложений, установленных на устройстве (кроме системных приложений и Kaspersky Internet Security), 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 Kaspersky Internet Security нажмите **Мои приложения**.
2. Перейдите в раздел **Приложения**.
3. Разрешите Kaspersky Internet Security 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 Kaspersky Internet Security.

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

d. Возвратитесь в Kaspersky Internet Security.

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

[Просмотр установленных приложений]

1. В панели быстрого запуска Kaspersky Internet Security 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 Kaspersky Internet Security 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 Kaspersky Internet Security 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**.

Просмотр отчетов приложения

Kaspersky Internet Security постоянно формирует отчеты.

В отчетах вы можете просмотреть:

- информацию о работе Антивируса, например, результаты проверки, сведения о найденных угрозах, обновлении или изменениях параметров Антивируса;
- 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.

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 Анти-Вора и Блокировки приложений;
- приложения, заблокированные вами, с помощью функции Блокировка приложений;
- удаление Kaspersky Internet Security;
- 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 Анти-Вора 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 Анти-Вора.

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:

1. В окне с запросом секретного кода нажмите **Я не помню код**.
2. Введите пароль от вашей учетной записи 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 учетной записью, которая использовалась 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 на устройстве с Kaspersky Internet Security.
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 Kaspersky Internet Security и в системных настройках вашего устройства используются разные графические ключи.

Чтобы защитить доступ к функциям Kaspersky Internet Security,

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

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

3. Следуйте инструкциям мастера установки графического ключа.

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

Если вы забыли свой графический ключ, выполните следующие действия:

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

Об отпечатке пальца

Если вы уже установили секретный код, вы можете также добавить защиту от несанкционированного доступа с помощью отпечатка пальца. Kaspersky Internet Security 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 Kaspersky Internet Security, установите флажок **Доступ по отпечатку пальца** в мастере первоначальной настройки или нажмите **Настройки** > **Блокировка экрана**.

Использование приложения на часах

Подготовка к работе приложения на часах

Эта функция недоступна для устройств Huawei.

Вы можете использовать часы для получения уведомлений от Kaspersky Internet Security и для управления Kaspersky Internet Security. Для этого устройство должно быть подготовлено к работе с часами.

Чтобы начать использовать Kaspersky Internet Security на часах:

1. Обновите на устройстве приложение Google.
2. Установите на устройство приложение Android Wear.

   Подробнее об установке и обновлении приложений вы можете узнать на веб-сайте технической поддержки Google Play.

3. Выполните на часах возврат к заводским настройкам.

   Возврат к заводским настройкам необходимо выполнить, если часы были ранее соединены с другим устройством.

4. Подключите часы к вашему устройству.

Подробнее о подключении часов к устройству вы можете узнать на веб-сайте технической поддержки Android Wear.

Установка приложения на часы происходит в фоновом режиме.

Ваше устройство и часы готовы к использованию.

Удаление приложения с помощью часов

Чтобы удалить Kaspersky Internet Security с ваших часов, необходимо удалить приложение Kaspersky Internet Security с вашего устройства.

Подробнее об удалении приложения с устройства вы можете узнать в разделе Удаление приложения.

Управление с помощью голосовых команд

Вы можете выполнить действие в приложении Kaspersky Internet Security, передав голосовую команду с помощью часов.

Чтобы выполнять голосовые команды, ваше устройство должно быть подключено к интернету.

Голосовые команды, доступные в Kaspersky Internet Security, перечислены в таблице ниже.

Голосовые команды Kaspersky Internet Security

Голосовая команда	Содержание голосовой команды
проверить	Выполнить проверку устройства
обновить	Обновить базы приложения Kaspersky Internet Security
найти	Выполнить поиск телефона, включив на нем звуковой сигнал

Чтобы совершить действие с помощью голосовой команды, выполните следующие действия:

1. Нажмите на экран часов.
2. Смахните влево.

   Появится меню со списком приложений.
3. Найдите в списке приложений Kaspersky Internet Security и нажмите на него.
4. Нажмите на  .
5. Произнесите одну из перечисленных выше голосовых команд.

Команда будет выполнена.

Запуск проверки с помощью часов

Вы можете запустить проверку на устройстве с помощью часов.

Если на часы пришло уведомление о необходимости проверки, вы можете использовать его, чтобы запустить проверку. Также вы можете запустить проверку вручную.

Чтобы запустить проверку Kaspersky Internet Security с помощью уведомления, пришедшего на часы, выполните следующие действия:

1. Нажмите на экран часов.
2. Смахните вверх несколько раз, пока не увидите уведомление Kaspersky Internet Security о необходимости проверки.
3. Смахните влево.
4. Нажмите **Запустить проверку сейчас**.

На вашем устройстве начнется проверка.

Чтобы запустить проверку Kaspersky Internet Security вручную, выполните следующие действия:

1. Нажмите на экран часов.
2. Смахните влево.

   Появится меню со списком приложений.
3. Найдите в списке приложений Kaspersky Internet Security и нажмите на него.
4. Смахните влево.
5. Нажмите **Запустить проверку** или воспользуйтесь *голосовой командой* "проверить".

На вашем устройстве начнется проверка.

О результатах проверки вы можете узнать в приложении Kaspersky Internet Security на устройстве.

Запуск обновления с помощью часов

Вы можете запустить обновление баз приложения Kaspersky Internet Security с помощью часов.

Если на часы пришло уведомление о необходимости обновления, вы можете использовать его, чтобы запустить обновление. Также вы можете запустить обновление вручную.

Чтобы запустить обновление Kaspersky Internet Security с помощью уведомления, пришедшего на часы, выполните следующие действия:

1. Нажмите на экран часов.
2. Смахните вверх несколько раз, пока не увидите уведомление Kaspersky Internet Security о необходимости обновления.
3. Смахните влево.
4. Нажмите **Запустить обновление сейчас**.

На вашем устройстве начнется обновление баз приложения.

Чтобы запустить обновление Kaspersky Internet Security вручную, выполните следующие действия:

1. Нажмите на экран часов.
2. Смахните влево.

Появится меню со списком приложений.

3. Найдите в списке приложений Kaspersky Internet Security и нажмите на него.
4. Смахните влево.
5. Нажмите **Запустить обновление** или воспользуйтесь голосовой командой "*обновить*".

На вашем устройстве начнется обновление баз приложения Kaspersky Internet Security.

О результатах обновления вы можете узнать в приложении Kaspersky Internet Security на устройстве.

Поиск телефона с помощью часов

Вы можете выполнить поиск своего телефона с помощью часов, если вы не можете найти телефон, но предполагаете, что он находится в пределах слышимости.

Чтобы выполнить поиск телефона, выполните следующие действия:

1. Нажмите на экран часов.
2. Смахните влево.

   Появится меню со списком приложений.
3. Найдите в списке приложений Kaspersky Internet Security и нажмите на него.
4. Смахните влево.
5. Нажмите **Найти телефон** или воспользуйтесь голосовой командой "*найти*".

   Телефон подаст звуковой сигнал.
6. Нажмите на экран часов, чтобы прервать подачу звукового сигнала.

Использование My Kaspersky

О My Kaspersky

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

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

Вы можете зайти на My Kaspersky одним из следующих способов:

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

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

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

Об учетной записи My Kaspersky

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

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

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

Если введенный пароль слишком простой или распространенный, учетная запись не будет создана.

После создания учетной записи на указанный вами адрес электронной почты будет выслано сообщение, содержащее ссылку для активации вашей учетной записи.

Активируйте учетную запись по ссылке из сообщения.

О двухэтапной проверке

Двухэтапная проверка может быть недоступна в вашем регионе. Дополнительную информацию см. в справке My Kaspersky.

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

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

Код безопасности, отправленный в SMS-сообщении на номер вашего телефона, действителен в течение короткого периода. После его истечения вы можете запросить новый код.

Если вы не получили SMS-сообщение с кодом безопасности

1. Проверьте доступность мобильной сети.
2. Дождитесь, чтобы кнопка **Запросить код еще раз** стала активной.
3. Нажмите на кнопку **Запросить код еще раз**.

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

Управление Kaspersky Internet Security через My Kaspersky

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

- обновить антивирусные базы приложения;
- включить Постоянную защиту, если она была выключена;
- приобрести или обновить подписку на использование функций премиум-версии Kaspersky Internet Security;
- управлять функциями Анти-Вора: 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 учетной записью, которая использовалась 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.

Настройка уведомлений приложения

По умолчанию в Kaspersky Internet Security 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.

Ранний доступ к функциям

В бесплатной версии Kaspersky Internet Security 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

Способы получения технической поддержки

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

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

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

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

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

Источники информации о приложении

Страница Kaspersky Internet Security на сайте "Лаборатории Касперского"

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

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

Страница Kaspersky Internet Security 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 Kaspersky Internet Security, 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

Общие проблемы

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

Для приложения Kaspersky Internet Security известны следующие проблемы:

- На некоторых устройствах Блокировка приложений может работать некорректно в режиме разделенного экрана.
- На устройствах с операционной системой Android 6 если вы копируете вредоносное ПО в диспетчере файлов, Постоянная защита 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 работает некорректно на устройствах с Android версии 5 или более ранней.
- Kaspersky Internet Security не блокирует входящие спам-звонки на второй линии.
- На некоторых устройствах с кастомными прошивками MIUI и EMUI Защита от удаления может не работать в Kaspersky Internet Security. 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 4.2, 4.4 и 5.x 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 4.2, 4.4 и 5.x.
- На некоторых устройствах с Android 6.0 или более поздних Интернет-защита и Защита чатов могут не работать в режиме экономии заряда батареи. Сетевая активность блокируется для экономии заряда аккумулятора, поэтому Kaspersky Internet Security 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 Internet Security в список исключений для режима экономии заряда батареи.

- Kaspersky Internet Security несовместим с Xposed Framework.

  Для корректной работы Kaspersky Internet Security:

  1. Удалите Xposed Framework.
  2. Удалите Kaspersky Internet Security
  3. Установите Kaspersky Internet Security .
  4. Активируйте Kaspersky Internet Security .

- Во время установки Kaspersky Internet Security 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 Kaspersky Internet Security.

Если приведенные выше инструкции не помогли:

1. Удалите учетную запись Google со своего устройства. См. инструкции в справке Google.
2. Перезапустите устройство.
3. Добавьте учетную запись Google на свое устройство. См. инструкции в справке Google.
4. Попробуйте еще раз установить Kaspersky Internet Security.
5. Если проблема не исправлена, попробуйте обновить операционную систему до Android 5.0 или более поздних версий.

Устройства ASUS

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

- На устройствах с установленным Asus Mobile Manager, если после настройки Kaspersky Internet Security вы закроете это приложение в списке запущенных, Asus Mobile Manager может заблокировать автозапуск Kaspersky Internet Security. В результате, Kaspersky Internet Security 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 Kaspersky Internet Security в приложения, 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

Kaspersky Internet Security 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 корректной работы Kaspersky Internet Security.

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

Шаг 1. Исключите Kaspersky Internet Security 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 Internet Security** и нажмите на него.

   e. Выберите **Запретить** для **Kaspersky Internet Security**, 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 Internet Security** и нажмите на него.

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

Шаг 2. Закрепите Kaspersky Internet Security 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 **Kaspersky Internet Security** вниз. Появится значок  .
   - Для устройств с оболочкой EMUI 8.x выберите приложение **Kaspersky Internet Security** и нажмите на значок  .

Значок  показывает, что приложение запущено.

Шаг 3. Включите ручное управление способом запуска Kaspersky Internet Security

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 **Kaspersky Internet Security** и установите переключатель **Управлять всем автоматически** 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**.

Kaspersky Internet Security 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 Kaspersky Internet Security в приложения, 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.

Устройства Lenovo

Kaspersky Internet Security 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 Internet Security.
  3. Нажмите на значок замка рядом с названием приложения.

     Значок показывает, что приложение запущено.

Устройства Meizu

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

- Kaspersky Internet Security 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 Internet Security продолжать работу в спящем режиме.

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

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

- Kaspersky Internet Security может выгружаться из оперативной памяти устройства. Для корректной 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** > Kaspersky Internet Security > **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:

  Kaspersky Internet Security может не получить доступ к разрешениям на устройстве Meizu Pro 6 Plus с Android 6.0.1, поэтому приложение 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 Internet Security** > **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 Анти-Вора 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 Анти-Вор 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

Kaspersky Internet Security 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 Kaspersky Internet Security в приложения, 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.

Kaspersky Internet Security нельзя установить на эти устройства через Google Play.

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

Kaspersky Internet Security 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 Kaspersky Internet Security в приложения, 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, Постоянная защита 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 Internet Security может не запускаться после перезагрузки устройства. Чтобы решить эту проблему, разрешите автоматический перезапуск для Kaspersky Internet Security. Например, используйте приложение **Smart Manager**. Для этого нажмите **Smart Manager >ОЗУ > Прил.Автозагр.** и включите переключатель Kaspersky Internet Security.

  > 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 Internet Security помещено (пользователем или автоматически устройством) в список приложений, находящихся в режиме глубокого сна, основная функциональность приложения может быть потеряна. Для корректной работы приложения добавьте Kaspersky Internet Security 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 Kaspersky Internet Security в список **Никогда не спящие приложения** .

Устройства XIAOMI

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

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

Шаг 1. Выдайте Kaspersky Internet Security 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 **Kaspersky Internet Security** .
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 Kaspersky Internet Security 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 **Kaspersky Internet Security** вниз. Появится значок  .
- Выберите приложение **Kaspersky Internet Security** и нажмите на значок  .

Значок  показывает, что приложение запущено.

Kaspersky Internet Security 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 Internet Security** > **Нет ограничения**.

- Kaspersky Internet Security может не запускаться после перезагрузки устройства или выгрузки из оперативной памяти. Чтобы решить эту проблему, разрешите автоматический перезапуск для Kaspersky Internet Security 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 Kaspersky Internet Security в приложения, которые могут запускаться автоматически или запускать приложение вручную после перезагрузки устройства.
- Один из компонентов Интернет-защиты может не работать 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 Kaspersky Internet Security 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 Анти-Вор 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

Kaspersky Internet Security 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 Internet Security.
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 Internet Security** > **Не экономить**.

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

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

Юридическая 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.

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.

Информация для бета-тестировщиков

О бета-версии

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

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

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

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

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

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

Принять участие в бета-тестировании

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

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

Отправить отзыв

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

Завершить бета-тестирование

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

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

Бета-версия и подписки

Мы рекомендуем вам зарегистрировать отдельную учетную запись My Kaspersky, чтобы использовать ее исключительно для бета-тестирования.

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

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