

# Описание функционала приложения Kaspersky Security для МТС

## Оглавление

Краткое описание.....	2
<b>Раздел 1. Общая информация.</b> .....	2
1.1. Установка Kaspersky Security для МТС .....	2
1.2. Лицензия / Активация.....	2
1.2.1. О лицензии .....	2
1.2.2. Как активировать программу .....	2
1.2.3. Срок годности лицензии.....	3
1.2.4. Использование подписки других мобильных продуктов .....	3
1.3. Удаление Kaspersky Security для МТС .....	3
1.4. Системные требования для программы Kaspersky Security для МТС:.....	3
<b>Раздел 2. Бесплатная версия приложения.</b> .....	3
2.1. Сканер .....	4
2.2. Анти-Вор.....	4
2.2.1. Дистанционный поиск и блокировка мобильного устройства.....	5
2.2.2. Дистанционное включение сирены на мобильном устройстве .....	5
2.2.3. Дистанционное удаление данных с устройства.....	5
2.2.4. Дистанционное фотографирование.....	6
2.3. Фильтр вызовов и SMS .....	6
2.3.1. Режимы работы:.....	6
2.3.2. Как добавить запись в список запрещенных контактов:.....	7
2.3.3. Как отредактировать запись в списке: .....	7
<b>Раздел 3. Коммерческая версия приложения.</b> .....	7
3.1. Антивирус.....	8
3.1.1. Настройка режима защиты .....	8
3.1.2. Выбор типа защищаемых файлов.....	8
3.2. Личные контакты .....	9
3.2.1. Скрытие Личных контактов вручную .....	9
3.2.2. Автоматическое сккрытие Личных контактов.....	10
3.3. Веб-фильтр и SMS Анти - Фишинг.....	10
<b>Раздел 4. Пробная версия приложения.</b> .....	10
<b>Дополнительно</b> .....	11

## Краткое описание

Kaspersky Security для МТС – это мобильное приложение, позволяющее обеспечить безопасность Вашего мобильного устройства, а именно: защита от вирусов и угроз в сети, фильтрация нежелательных вызовов и sms - сообщений, защита от воров и ряд дополнительных функций.

Приложение доступно в трех вариантах, различающихся набором функциональных возможностей.

## Раздел 1. Общая информация.

### 1.1. Установка Kaspersky Security для МТС

Установка мобильного приложения Kaspersky Security для МТС может быть произведена следующими способами:

- Самостоятельная загрузка приложения из Android-Market
- Самостоятельная загрузка со страницы приложения

### 1.2. Лицензия / Активация.

#### 1.2.1. О лицензии

Лицензия – это право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО «Лаборатория Касперского», в котором указано, на каких условиях вы можете использовать программу.

**Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.**

Считается, что вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения при установке программы или первом открытии программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы или не использовать программу.

Лицензия включает в себя право на получение следующих видов услуг:

- Использование программы на одном устройстве.
- Обращение в Службу технической поддержки «Лаборатории Касперского».
- Получение прочих услуг, предоставляемых вам «Лабораторией Касперского» или ее партнерами в течение срока действия лицензии. Объем предоставляемых услуг и срок использования программы зависят от версии программы

#### 1.2.2. Как активировать программу

Вы можете выбрать один из следующих вариантов активации **Kaspersky Security для МТС**:

- **Бесплатная версия – ограниченный функционал**  
активируется автоматически при установке программы, если вы не активировали подписку для коммерческой версии. Бесплатная версия включает в себя функции **Сканер, Анти-Вор и Фильтр вызовов и SMS** и не ограничена по времени использования. С бесплатной версии вы можете перейти на пробную версию или полную Коммерческую версию программы.
- **Пробная версия – полный функционал**  
Позволяет использовать все функции программы в течение ознакомительного периода (7 дней). Активация пробной версии возможна после установки программы, кроме случаев, когда пробная версия была использована ранее или используется в данный момент. После окончания пробной версии вы можете перейти на полную Коммерческую версию или бесплатную версию программы. По истечении ознакомительного периода программа автоматически переключится на бесплатную версию.
- **Коммерческая версия – полный функционал**  
Предоставляет доступ ко всем функциям программы по модели подписки. Модель подписки означает, что каждые 30 дней будут осуществляться списания за использование приложения.

Для активации коммерческой версии необходимо оформить подписку с помощью кнопки «Подписаться». Для активации подписки необходим доступ в интернет.

### 1.2.3. Срок годности лицензии


Срок годности у Лицензии, которая не была активирована ни разу, отсутствует. Лицензия будет действительна сколько угодно времени до тех пор, пока не будет произведена первая активация пробной или Коммерческой версии. С момента первой активации пробной или Коммерческой версии начинается отсчет срока лицензии продукта.

### 1.2.4. Использование подписки других мобильных продуктов

Использование кодов активации других продуктов, например, Kaspersky Tablet Security (Android OS) или Kaspersky Mobile Security (Android), для активации продукта Kaspersky Security для МТС – **невозможно**.

## 1.3. Удаление Kaspersky Security для МТС

Чтобы удалить **Kaspersky Security для МТС** с вашего устройства, выполните следующие действия:

1. В главном окне программы раскройте панель быстрого запуска (для этого нажмите на кнопку ) и нажмите **Настройка**.
2. Нажмите **Дополнительные параметры -> Удаление программы**.
3. В окне **Kaspersky Security для МТС** нажмите **Далее**. Введите секретный код и нажмите **Вход**.
4. В окне **Kaspersky Security для МТС** нажмите **Далее**.
5. Программа **Kaspersky Security для МТС** удалена с вашего устройства.

Если вы настраивали **Анти-Вор** или **Личные контакты**, то для удаления **Kaspersky Security для МТС** вам понадобится секретный код. Если вы забыли секретный код, воспользуйтесь процедурой восстановления.

### 1.4. Системные требования для программы Kaspersky Security для МТС:

- Смартфон или планшет, работающий под управлением ОС Android версий 2.3 – 5.x, Android Lollipop и Android 6.0 Marshmallow
- Разрешение экрана от 320x480 пикселей.
- 65 МБ свободного места в основной памяти устройства.
- Архитектура процессора Intel Atom x86, ARM5, ARM6 или ARM7.

Для использования функций **Фильтр вызовов и SMS**, **Личные контакты**, **SIM-Контроль**, **SMS Анти-Фишинг**, а также для приема и отправки SMS-команд нужна установленная в устройство SIM-карта.

Программа была протестирована на следующих мобильных устройствах:

- Acer Iconia Tab A501, A101.
- Google Nexus S, Nexus X, Nexus 4, Nexus 5, Nexus 10 (Tablet).
- HTC OneX, Incredible S.
- Huawei T2; Huawei U8650.
- LG Optimus G.
- Motorola Xoom, Razr HD.
- Samsung Galaxy Note; Note 2.
- Samsung Galaxy S; S2; S3; S4.
- Samsung Galaxy Tab; 10.1.
- Sony Ericsson Xperia Arc, x10, x26.

Программа несовместима со следующими мобильными устройствами:

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

## Раздел 2. Бесплатная версия приложения.

В данной версии приложения доступны следующие функции.

## 2.1. Сканер

С помощью Сканера можно проверять на наличие угроз все устройство, установленные программы или выбранную папку, настроить проверку устройства по расписанию, а также обновлять антивирусные базы, обеспечивающие актуальную защиту ваших данных.

В платной версии программы компонент «Сканер» называется «Антивирус». При этом «Антивирус» имеет ряд дополнительных к «Сканеру» функций.

### 2.1.1. Функционал «Сканер»:

#### 1. Полная проверка устройства:

- включает в себя проверку всей файловой системы устройства на наличие вирусов и вредоносных программ. Рекомендуется сделать такую проверку хотя бы один раз после установки приложения «Kaspersky Security для МТС», чтобы убедиться в сохранности данных;
- Как запустить: в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Проверка – Полная проверка».

#### 2. Быстрая проверка:

- проверка установленных на устройстве программ (без проверки всей файловой системы);
- Как запустить: в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Проверка – Быстрая проверка».

#### 3. Проверка файлов и папок:

- Выборочная проверка папок или файлов во встроенной памяти устройства или на карте памяти (перечень проверяемых файлов/папок определяет пользователь);
- Как запустить: в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Проверка – Проверка папки», далее выбрать папку или файл.

#### 4. Автоматическая проверка по расписанию:

- Автоматический запуск полной проверки мобильного устройства по расписанию (с заданной периодичностью либо в конкретные день и время);
- Как запустить: в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Настройка – Антивирус – Параметры проверки». Далее задать периодичность запуска (параметр «Расписание») либо день и время запуска (параметры «День запуска» и «Время запуска»).

### 2.1.2. Обновление антивирусных баз и версий программы

Для корректной работы приложения необходимо регулярно обновлять антивирусные базы и версии программы.

В бесплатной версии приложения обновление антивирусных баз и версии приложения производится вручную пользователем. Для этого необходимо в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Обновление».

Для обновления на мобильном устройстве должно быть настроено соединение с интернетом.

## 2.2. Анти-Вор

Компонент Анти-Вор в Kaspersky Security для МТС предназначен для защиты хранящихся на устройстве данных от несанкционированного доступа к ним и поиска устройства в случае его кражи или потери.

Для дистанционного запуска возможностей **Анти-Вора** необходимо, чтобы «Kaspersky Security для МТС» установлен в качестве администратора мобильного устройства, на котором будут производиться удаленные действия, чтобы устройство принимало сигналы сотовой связи, а также чтобы дистанционная активация данных функцией была разрешена в настройках.

Все функции **Анти-Вора** включаются автоматически после первоначальной настройки с параметрами, рекомендованными специалистами **Лаборатории Касперского**. Контроль действий с SIM-картой доступен только на устройствах с установленной SIM-картой.

Для использования каждой функции **Анти-Вора** нужно ввести секретный код, заданный при первом

запуске **Анти-Вора** или **Личных контактов**.

Запустить функции **Анти-Вора** можно удаленно с любого мобильного устройства при помощи специальных SMS-команд или через веб-портал <https://anti-theft.kaspersky.com>.

Передача данных с потерянного устройства (например, координат устройства при использовании функции **Блокирование** и **Поиск**) происходит путем отправки платного SMS-сообщения на сервер **Лаборатории Касперского**. Стоимость SMS-сообщения зависит от региона, в котором вы находитесь, и определяется вашим оператором сотовой связи.

Возможности «Анти - Вор»:

### 2.2.1. Дистанционные поиск и блокировка мобильного устройства

Чтобы заблокировать свое устройство и получить координаты его местоположения на карте через web-портал, нужно:

- Открыть портал <https://anti-theft.kaspersky.com> на любом устройстве;
- На закладке с названием того устройства, которое нужно найти/заблокировать нажать кнопку «Блокирование и поиск» (при необходимости можно задать текст, который будет выводиться на экране потерянного устройства), также укажите адрес электронной почты, на которой Вы хотите получать информацию о потерянном устройстве;
- Нажмите кнопку «заблокировать и найти»;
- Когда устройство будет найдено, его координаты появятся на портале, также они будут отправлены на указанный адрес электронной почты.

При отсутствии возможности воспользоваться web – порталом можно отправить SMS с другого мобильного устройства на то мобильное устройство, которое потеряно/украдено и на котором установлено приложение «Kaspersky Security для МТС» с текстом «find: <код>» (где «код» - это секретный код «Kaspersky Security для МТС» на потерянном/украденном устройстве).

### 2.2.2. Дистанционное включение сирены на мобильном устройстве

Функционал позволяет включить сирену на устройстве, даже если звук на устройстве выключен, а также заблокировать устройство дистанционно.

- Открыть портал <https://anti-theft.kaspersky.com> на любом устройстве;
- На закладке с названием того устройства, которое нужно заблокировать и на котором включить сирену и нажмите на кнопку «Сирена» (при необходимости можно задать текст, который будет выводиться на экране одновременно с включением сирены);
- Нажмите кнопку «включить сирену»;

При отсутствии возможности воспользоваться web – порталом можно отправить SMS с другого мобильного устройства на то мобильное устройство, которое потеряно/украдено и на котором установлено приложение «Kaspersky Security для МТС» с текстом «find: <alarm>» (где «код» - это секретный код «Kaspersky Security для МТС» на потерянном/украденном устройстве).

### 2.2.3. Дистанционное удаление данных с устройства

Данный функционал позволяет удалить персональные данные (контакты, переписку, данные об учетной записи Google) и данные на карте памяти, либо вернуть устройство к заводским настройкам.

- Открыть портал <https://anti-theft.kaspersky.com> на любом устройстве;
- На закладке с названием того устройства, на котором нужно удалить данные, нажмите кнопку «Удаление данных», далее выберите. Какие именно данные нужно удалить:
  - Чтобы удалить персональные данные (учетная запись Google, переписка, контакты) – нажмите «Только личная информация»;
  - Чтобы удалить все данные, включая данные с карты памяти, и вернуть устройство к заводским настройкам, нажмите «Все данные с устройства».
- Внимание: после удаления всех данных приложение «Kaspersky Security для МТС» также будет удалено – дальнейшие удаленные действия с утерянным/украденным мобильным устройством станут невозможны.

При отсутствии возможности воспользоваться web – порталом можно отправить SMS с другого мобильного устройства на то мобильное устройство, которое потеряно/украдено и на котором установлено приложение «Kaspersky Security для МТС» с текстом:

- «w!re: <код>» (удаление персональных данных и данных с карты памяти);
- «w!re: <код>» (удаление всех данных и возврат к заводским настройкам);

#### 2.2.4. Дистанционное фотографирование

Функционал позволяет дистанционно получить фотографию человека, который использует потерянное устройство, а также удаленно заблокировать устройство.

Функция доступна только для мобильных устройств с фронтальной камерой.

- Открыть портал <https://anti-theft.kaspersky.com> на любом устройстве;
- На закладке с названием того устройства, с которого нужно получить фото и которое нужно заблокировать, нажмите кнопку «тайное фото» (также можно добавить текст, который будет выведен на экран заблокированного устройства);
- Нажмите «получить фото».

После выполнения команды фотографии будут доступны на web-портале.

### 2.3. Фильтр вызовов и SMS

**Фильтр вызовов и SMS** позволяет блокировать нежелательные входящие вызовы и SMS с помощью режимов фильтрации на основе списков разрешенных и запрещенных контактов. Для этого необходимо сформировать список контактов и задать правила обработки входящих вызовов и SMS.

**Фильтр вызовов и SMS** доступен только на устройствах с установленной SIM-картой.



#### 2.3.1. Режимы работы:

- **Стандартная фильтрация контактов:**
  - получение звонков и sms от разрешенных контрактов и блокировка звонков и sms от запрещенных контактов. При получении SMS-сообщения или вызова с номера, не занесенного ни в один из списков, предлагает выбрать, как следует поступать со звонками и sms от этого номера. Данный режим установлен по умолчанию;
  - как настроить: в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Фильтр вызовов и sms – Режим фильтра вызовов и sms – Стандартный».
- **Блокирование всех контактов, кроме разрешенных:**
  - разрешается прием SMS-сообщений и вызовов от номеров только из списка разрешенных контактов. Все остальные SMS-сообщения и вызовы блокируются.
  - как настроить: в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Фильтр вызовов и sms – Режим фильтра вызовов и sms – Разрешенные контакты».
  - Если нужно разрешить получение звонков от номеров из телефонной книги, в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Настройка – Фильтр вызовов и sms», далее установить флажок «Разрешать Контакты».
- **Блокирование только запрещенных контактов:**
  - разрешается прием SMS-сообщений и вызовов от номеров только из списка разрешенных контактов. Все остальные SMS-сообщения и вызовы блокируются.
  - как настроить: в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Фильтр вызовов и sms – Режим фильтра вызовов и sms – Запрещенные контакты»;
  - если требуется запретить получение sms с номеров, содержащих буквы, в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Настройки – Фильтр вызовов и sms», далее установить флажок «Блокировать нечисловые номера».
- **Отключен** — фильтрация SMS-сообщений и вызовов не выполняется.

1. Если вы выбрали режим **Запрещенные контакты**, будет автоматически активирована функция **Блокировать нечисловые номера**: запрет входящих вызовов и SMS с номеров, содержащих буквенные символы.

2. Если вы выбрали режим **Стандартный**, будут автоматически активированы функции **Разрешать контакты** и **Блокировать нечисловые номера**.

#### 2.3.2. Как добавить запись в список запрещенных контактов:

1. В главном окне программы раскройте панель быстрого запуска (для этого нажмите на кнопку ) и нажмите Настройка.
2. Выберите Фильтр вызовов и SMS --> Запрещенные контакты --> Добавить.
3. В окне «запрещать входящие» выберите тип входящей информации, которую надо запретить: SMS, Вызовы, Вызовы и SMS.
4. В поле Запрещенный номер телефона введите нужный номер. Чтобы выбрать номер из списка контактов, нажмите на кнопку . Если на предыдущем шаге вы выбрали вариант запрещать входящие SMS, в поле Запрещенный текст введите текст, при обнаружении которого Фильтр вызовов и SMS будет блокировать сообщение.
5. Нажмите Сохранить.

#### 2.3.3. Как отредактировать запись в списке:

- Чтобы изменить запись в списке, нажмите на нее и в окне **Запрещенные контакты** выберите **Изменить**. Изменив запись, нажмите **Сохранить**.
- Чтобы удалить запись, нажмите на нее и в окне **Запрещенные контакты** выберите **Удалить**.
- Чтобы удалить все записи, нажмите на любую запись, в окне **Запрещенные контакты** выберите **Удалить все** и подтвердите удаление, нажав **Да**.

### Раздел 3. Коммерческая версия приложения.

В данной версии приложения доступны все функции из Бесплатной версии (Сканер, Анти – Вор, Фильтра вызовов и SMS), а также ряд дополнительных функций.

### 3.1. Антивирус

Для защиты вашего устройства от вирусов и других вредоносных программ используется компонент Антивирус (в бесплатной версии данный компонент называется «Сканер»).

Антивирус содержит всю функциональность Сканера, а также выполняет следующие действия:

- защищает ваше устройство в режиме реального времени;
- проверяет новые установленные программы до их первого запуска, используя антивирусные базы и облачный онлайн-сервис Kaspersky Security Network;
- позволяет автоматически обновлять антивирусные базы.

В **Kaspersky Security для МТС** вы можете выбрать режим защиты, подключить «облачную» защиту, а также настроить параметры проверки устройства.

#### 3.1.1. Настройка режима защиты


Kaspersky Security для МТС начинает защищать ваше устройство при старте операционной системы и постоянно находится в оперативной памяти.

Защита доступна только при оформлении подписки.

Предлагаются следующие режимы защиты:

- **Расширенный** — проверка файлов при любом действии с ними, а также проверка новых программ сразу после их установки. При этом режиме защиты вы можете дополнительно выбрать типы файлов, которые будут проверяться на наличие угроз, а также определить действие программы при обнаружении угрозы.
- **Рекомендуемый** — проверка только новых программ (один раз, сразу после их установки). Этот режим установлен по умолчанию.
- **Отключен**.

Вы можете выбрать подходящий режим защиты, для этого выполните следующие действия:

1. В главном окне программы раскройте панель быстрого запуска (для этого нажмите на кнопку ) и нажмите **Настройка**.
2. В окне **Режим защиты** выберите подходящий режим.

#### 3.1.2. Выбор типа защищаемых файлов

По умолчанию **Kaspersky Security для МТС** не следит за файлами, используемыми другими программами, ограничиваясь проверкой новых установленных программ.

При включении расширенного режима защиты Kaspersky Security для МТС проверяет все файлы на устройстве во время их использования другими программами или пользователем.

Вы можете указать тип файлов, которые Kaspersky Security для МТС будет проверять на наличие вредоносных объектов. Для этого выполните следующие действия:

1. В окне **Антивирус** убедитесь, что в блоке **Режим защиты** установлено **расширенная**. Нажмите **Защита**.
2. Нажмите **Тип проверяемых файлов** и укажите нужный тип:
  - **Все файлы** — в этом случае проверяться будут все файлы, включая документы, архивы, видео- и аудиофайлы, исполняемые файлы. Этот вариант выбран по умолчанию.
  - **Только исполняемые** — в этом случае проверяться будут только исполняемые файлы программ.

#### 3.1.3. Выбор действия при обнаружении угрозы

По умолчанию Kaspersky Security для МТС удаляет обнаруженные угрозы.

Вы можете задать действие, которое программа будет выполнять при обнаружении вредоносного объекта, для этого выполните следующие действия:

1. В окне **Антивирус** убедитесь, что в блоке **Режим защиты** установлено **расширенная**. Нажмите **Защита**.
2. Нажмите **Действие при обнаружении угрозы** и выберите действие:
  - **На карантин** — обнаруженный файл будет помещен на карантин.
  - **Удалить** — обнаруженный файл будет удален без уведомления пользователя.



- Специалисты **Лаборатории Касперского** рекомендуют использовать это действие.
- **Пропустить** — к обнаруженному файлу не будет применено никаких действий.

#### 3.1.4. Облачная защита


В **Kaspersky Security для МТС** реализован «облачный» механизм антивирусной защиты. Суть механизма состоит в том, что при возникновении потенциальной угрозы (например, при установке неизвестного приложения) **Kaspersky Security для МТС** проверяет репутацию приложения в облачной сети **Kaspersky Security Network**.

Более подробную информацию о работе «облачных» антивирусных технологий вы найдете в статье на сайте <http://securelist.com>.

Участие пользователей в **Kaspersky Security Network (KSN)** позволяет **Лаборатории Касперского** оперативно собирать информацию о новых угрозах, разрабатывать способы их нейтрализации, тем самым повышая уровень защиты пользователей. Чем больше пользователей участвуют в **KSN**, тем надежнее становится защита для всех участников.

Облачная защита доступна, если выбран режим защиты **Рекомендуемый** или **Расширенный**, и по умолчанию включена.

Чтобы выключить/включить облачную защиту в **Kaspersky Security для МТС**, выполните следующие действия:

1. В главном окне программы раскройте панель быстрого запуска (для этого нажмите на кнопку ) и нажмите **Настройка**.
2. Нажмите **Антивирус**.
3. В окне **Антивирус** в блоке **Настройка** установите/снимите флажок **Проверка в облаке**.

#### 3.1.5. Автоматическое обновление по расписанию

Чтобы настроить автоматические обновления, нужно сделать следующее: в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Настройка – Антивирус – Обновление», далее настроить периодичность запуска обновления (параметр «Расписание») либо установить конкретные день и время проверки (параметры «День запуска» и «Время запуска»).

Для обновления на мобильном устройстве должно быть настроено соединение с интернетом.

Для автоматического обновления в выбранное время необходимо, чтобы мобильное устройство в тот момент было включено.

## 3.2. Личные контакты

Компонент **Личные контакты** в составе **Kaspersky Security для МТС** позволяет управлять защитой персональных данных. Предлагаются следующие возможности:

- Формирование списка скрываемых контактов, в которых перечислены конфиденциальные номера;
- Скрытие информации о контактах в телефонной книге, в прочитанных входящих sms, переданных и черновиках sms, а также записи о контактах в журнале вызовов;
- Блокировка сигналов о получении sms и входящих вызовов с конфиденциальных номеров («звонящий получает сигнал «занято»).

Чтобы сформировать список «Личных контактов» в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажмите «Личные контакты – Скрываемые контакты – Добавить», далее установите переключатель «Личные контакты» в состояние «Включено».

Вы можете настроить скрытие личных данных автоматически или вручную. Для этого выполните следующие действия:


#### 3.2.1. Скрытие Личных контактов вручную

Компонент **Личные контакты** запускается вручную. По умолчанию он отключен. Компонент может работать в одном из следующих режимов:

- **Конфиденциальная информация отображается** — защита конфиденциальных данных

отключена. Параметры **Личных контактов** доступны для изменения.


- **Конфиденциальная информация скрыта** — защита конфиденциальных данных включена. Компонент скрывает данные, которые связаны с защищенными контактами. Параметры **Личных контактов** недоступны для изменения.

Чтобы скрыть/отобразить **Личные контакты**, выполните следующие действия: В главном окне программы раскройте панель быстрого запуска (для этого нажмите на кнопку ) и нажмите **Личные контакты** -> **Личные контакты**.

### 3.2.2. Автоматическое скрывание Личных контактов

По умолчанию автоматическое скрывание **Личных контактов** отключено. Вы можете включить эту функцию и задать интервал времени, по истечении которого личные данные будут скрыты. Отсчет времени начинается в момент перехода устройства в режим энергосбережения.

Для задания нужного интервала выполните следующие действия:

1. В главном окне программы раскройте панель быстрого запуска (для этого нажмите на кнопку ) и нажмите **Настройка**.
2. Выберите **Личные контакты**. Введите секретный код и нажмите **Вход**.
3. Нажмите **Настройка** --> **Автоматическое скрывание**.
4. Выберите один из интервалов времени, по истечении которого личные данные будут скрыты: **Отключено (по умолчанию), Сразу, Через 5 минут, Через 10 минут, Через 15 минут, Через 30 минут**.

### 3.3. Веб-фильтр и SMS Анти - Фишинг

Веб – фильтр блокирует вредоносные сайты, цель которых – распространить вредоносный код, а также поддельные (фишинговые) веб – сайты, цель которых - украсть персональные данные или получить доступ к финансовым счетам. Веб – фильтр проверяет веб-сайты до открытия и блокирует те из них, которые считаются вредоносными или фишинговыми.

SMS Анти – фишинг блокирует ссылки в sms на вредоносные и поддельные веб –сайты.

**Веб-фильтр** проверяет веб-сайты только в стандартном браузере операционной системы и не проверяет их в других браузерах. Начиная с версии **Android 4.2.x** браузер **Google Chrome** считается стандартным браузером. В более ранних версиях системы стандартным браузером является **Android Browser**.

Как настроить:

1. Чтобы **настроить постоянную проверку веб – сайтов**, в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Настройка – Веб – фильтр», далее установить переключатель №Веб – фильтр» в положение «Включен». Если используется не стандартный браузер Android, а иной, то нажмите «Изменить браузер», далее следуйте указаниям мастера.
2. Чтобы настроить постоянную проверку ссылок в sms, в главном окне «Kaspersky Security для МТС» в панели быстрого запуска нажать «Настройка – Веб – фильтр», далее установить переключатель «SMS Анти – фишинг» в положение «Включен».

## Раздел 4. Пробная версия приложения.

В данной версии приложения на ограниченный срок доступны все функции из бесплатной и платной версий приложения: Сканер, Анти – Вор, Фильтра вызовов и SMS, Антиспам, Личные контакты, Веб – фильтр.

Срок использования – 7 дней.

По истечении данного срока, если пользователь самостоятельно не перешел на коммерческую версию продукта, приложение переводится в режим бесплатной версии, т.е. происходит ограничение функционала.

#### **Дополнительно**

При первоначальной настройке **Анти-Вора** либо при первом запуске **Личных контактов** в **Kaspersky Internet Security для Android** вам будет предложено ввести секретный код.

Секретный код потребуется вам в следующих случаях:

1. Доступ к параметрам Анти-Вора и Личных контактов.

2. При отправке SMS-команд удаленного запуска следующих функций: Блокирование и поиск устройства, Удаление персональных данных, Сирена, Скрытие личных контактов.
3. При удалении программы.

Специалисты **Лаборатории Касперского** рекомендуют использовать секретный код, состоящий не менее чем из семи цифр. Минимальное количество символов секретного кода составляет четыре цифры.

Не забывайте и не теряйте секретный код. В случае утраты секретного для **Kaspersky Internet Security для Android** воспользуйтесь процедурой восстановления.

Чтобы безопасно восстановить секретный код программы, выполните следующие действия:

1. Откройте веб-портал <https://anti-theft.kaspersky.com> на любом устройстве.
2. Войдите на веб-портал с помощью вашей учетной записи Kaspersky Account, которую вы использовали при первоначальной настройке программы. Если вы забыли пароль, вы можете его восстановить.
3. Выберите закладку с названием того устройства, для которого вам требуется восстановить секретный код.
4. Нажмите на кнопку Восстановление секретного кода. На веб-портале отобразится код восстановления.
5. Запустите Kaspersky Internet Security на устройстве.
6. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите Настройка > Анти-Вор.
7. При запросе ввести секретный код нажмите Меню > Восстановление секретного кода.
8. Введите код восстановления, указанный на веб-портале. На экране устройства отобразится ваш секретный код.
9. Введите ваш восстановленный секретный код.