

Kaspersky Mobile Security

**KASPERSKY** **lab**

Руководство пользователя

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью ЗАО «Лаборатория Касперского» (далее также «Лаборатория Касперского») и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения «Лаборатории Касперского».

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу <http://www.kaspersky.ru/docs>.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, «Лаборатория Касперского» ответственности не несет.

Дата редакции документа: 3/6/2013

© ЗАО «Лаборатория Касперского», 2013

<http://www.kaspersky.ru>  
<http://support.kaspersky.ru>

# СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ .....	5
В этом документе .....	5
Условные обозначения .....	6
ИСТОЧНИКИ ИНФОРМАЦИИ О ПРОГРАММЕ .....	8
Источники информации для самостоятельного поиска .....	8
Обсуждение программ «Лаборатории Касперского» на форуме .....	9
Обращение в Департамент продаж .....	9
Обращение в Отдел локализации и разработки технической документации .....	9
KASPERSKY MOBILE SECURITY .....	10
Что нового .....	11
Аппаратные и программные требования .....	11
Комплект поставки .....	12
Сервис для пользователей .....	12
ИНТЕРФЕЙС ПРОГРАММЫ .....	13
Значок в области уведомлений .....	13
Главное окно Kaspersky Mobile Security .....	13
Виджет для главного экрана устройства .....	15
Уведомления .....	16
ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ .....	17
О Лицензионном соглашении .....	17
О лицензии .....	17
О коде активации .....	18
ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ .....	19
РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ .....	20
Как активировать коммерческую версию программы .....	21
Как приобрести лицензию или продлить срок ее действия .....	21
Как посмотреть информацию о лицензии, узнать срок ее действия .....	22
Как проверить всю файловую систему устройства на вирусы .....	22
Как проверить на вирусы оперативную память устройства, папку или файл .....	23
Как настроить автоматический запуск проверки всего устройства на вирусы .....	23
Как обновить антивирусные базы и версию программы .....	23
Как настроить автоматическое обновление антивирусных баз и версий программы по расписанию .....	24
Как скрывать контакты и связанную с ними информацию .....	24
Как дистанционно с другого устройства скрыть контакты и связанную с ними информацию .....	25
Что такое Kaspersky Account .....	26
Как добавить устройство в мою учетную запись на веб-портале .....	26
Что делать, если устройство потеряно или украдено .....	26
Как отправить SMS-команды с другого устройства, на котором установлена Kaspersky Mobile Security .....	28
Как разрешить или запретить дистанционно запускать функции Анти-Вора на устройстве .....	28
Как при замене SIM-карты узнать новый номер телефона и заблокировать устройство .....	30
Как дистанционно заблокировать устройство и узнать его местоположение .....	30
Как дистанционно включить сирену на устройстве .....	31
Как удалить персональные данные с устройства или полностью отформатировать его .....	32

Как получить фотографии человека, который сейчас использует ваше устройство.....	33
Как избавиться от нежелательных вызовов и SMS.....	34
Как защитить персональные данные от кражи в сети.....	35
Как посмотреть отчеты о работе программы.....	36
Как изменить секретный код программы.....	36
Как восстановить секретный код программы.....	36
ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ.....	37
Способы получения технической поддержки .....	37
Техническая поддержка по телефону .....	37
Получение технической поддержки через Личный кабинет .....	38
ГЛОССАРИЙ.....	40
ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО» .....	42
ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ .....	43
УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ .....	44
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ .....	45

# ОБ ЭТОМ РУКОВОДСТВЕ

Этот документ представляет собой Руководство пользователя Kaspersky Mobile Security.

Руководство пользователя адресовано пользователям Kaspersky Mobile Security, которые знакомы с интерфейсом используемой операционной системы, владеют основными приемами работы в ней и умеют работать с интернетом.

Руководство пользователя предназначено для следующих целей:

- Познакомить с интерфейсом программы.
- Обеспечить быстрый поиск информации для решения типовых вопросов, связанных с работой Kaspersky Mobile Security.
- Рассказать о дополнительных источниках информации о программе и способах получения технической поддержки.

## В ЭТОМ РАЗДЕЛЕ

---

В этом документе ..... [5](#)

Условные обозначения ..... [6](#)

## В ЭТОМ ДОКУМЕНТЕ

В это руководство включены следующие разделы.

### Источники информации о программе

Этот раздел содержит описание источников информации о программе и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

### Kaspersky Mobile Security

Этот раздел содержит описание возможностей программы, а также краткую информацию о функциях и компонентах программы. Вы узнаете о том, из чего состоит комплект поставки и какие услуги доступны зарегистрированным пользователям программы. В разделе приведена информация о том, каким программным и аппаратным требованиям должно отвечать устройство, чтобы на него можно было установить программу.

### Интерфейс программы

Этот раздел содержит информацию об основных элементах графического интерфейса программы: значке программы, главном окне, окне настройки, виджете и окнах уведомлений.

### Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с активацией программы. Из этого раздела вы узнаете о назначении Лицензионного соглашения, типах лицензии, способах активации программы, а также о продлении срока действия лицензии.

## Запуск и остановка программы

Этот раздел содержит информацию о том, как запустить программу и как завершить работу с ней.

## Решение типовых задач

Этот раздел содержит пошаговые инструкции для выполнения основных задач пользователя, которые решает программа.

## Обращение в Службу технической поддержки

Этот раздел содержит сведения о способах обращения в Службу технической поддержки «Лаборатории Касперского».

## Глоссарий

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

## ЗАО «Лаборатория Касперского»

Этот раздел содержит информацию о ЗАО «Лаборатория Касперского».

## Информация о стороннем коде

Этот раздел содержит информацию о стороннем коде, используемом в программе.

## Уведомления о товарных знаках

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

## Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

# УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Текст документа сопровождается смысловыми элементами, на которые мы рекомендуем вам обращать особое внимание, – предупреждениями, советами, примерами.

Для выделения смысловых элементов используются условные обозначения. Условные обозначения и примеры их использования приведены в таблице ниже.

Таблица 1. Условные обозначения

ПРИМЕР ТЕКСТА	ОПИСАНИЕ УСЛОВНОГО ОБОЗНАЧЕНИЯ
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. В предупреждениях содержится информация о возможных нежелательных действиях, которые могут привести к потере информации, сбоям в работе оборудования или операционной системы.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания могут содержать полезные советы, рекомендации, особые значения параметров или важные частные случаи в работе программы.

ПРИМЕР ТЕКСТА	ОПИСАНИЕ УСЛОВНОГО ОБОЗНАЧЕНИЯ
<p><b>Пример:</b></p> <p>...</p>	<p>Примеры приведены в блоках на желтом фоне под заголовком «Пример».</p>
<p>Обновление – это...</p> <p>Возникает событие <i>Базы устарели</i>.</p>	<p>Курсивом выделены следующие смысловые элементы текста:</p> <ul style="list-style-type: none"> <li>• новые термины;</li> <li>• названия статусов и событий программы.</li> </ul>
<p>Нажмите на кнопку <b>Включить</b>.</p>	<p>Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.</p>
<p>➔ <i>Чтобы настроить расписание задачи, выполните следующие действия:</i></p>	<p>Вводные фразы инструкций выделены курсивом и значком «стрелка».</p>
<p>&lt;Имя пользователя&gt;</p>	<p>Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.</p>
<p>Отправьте SMS на ваше устройство со следующим специальным текстом <code>find:</code> &lt;код&gt;.</p>	<p>Специальным стилем выделен текст SMS-команды.</p>

# ИСТОЧНИКИ ИНФОРМАЦИИ О ПРОГРАММЕ

Этот раздел содержит описание источников информации о программе и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

## В ЭТОМ РАЗДЕЛЕ

---

Источники информации для самостоятельного поиска.....	<a href="#">8</a>
Обсуждение программ «Лаборатории Касперского» на форуме.....	<a href="#">9</a>
Обращение в Департамент продаж.....	<a href="#">9</a>
Обращение в Отдел локализации и разработки технической документации.....	<a href="#">9</a>

## ИСТОЧНИКИ ИНФОРМАЦИИ ДЛЯ САМОСТОЯТЕЛЬНОГО ПОИСКА

Вы можете использовать следующие источники для самостоятельного поиска информации о программе:

- страница на веб-сайте «Лаборатории Касперского»;
- страница на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Техническая поддержка по телефону» на стр. [37](#)).

Для использования источников информации на веб-сайте «Лаборатории Касперского» необходимо подключение к интернету.

### Страница на веб-сайте «Лаборатории Касперского»

Веб-сайт «Лаборатории Касперского» содержит отдельную страницу для каждой программы.

На странице ([http://www.kaspersky.ru/kaspersky\\_mobile\\_security](http://www.kaspersky.ru/kaspersky_mobile_security)) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница <http://www.kaspersky.ru> содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

## Страница на веб-сайте Службы технической поддержки (База знаний)

База знаний – раздел веб-сайта Службы технической поддержки, содержащий рекомендации по работе с программами «Лаборатории Касперского». База знаний состоит из справочных статей, сгруппированных по темам.

На странице программы в Базе знаний <http://www.kaspersky.ru/support/mobile/kms9and> вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи могут отвечать на вопросы, которые относятся не только к Kaspersky Mobile Security, но и к другим программам «Лаборатории Касперского», а также могут содержать новости Службы технической поддержки.

## Электронная справка

В состав электронной справки программы входят файлы контекстной справки.

Контекстная справка содержит сведения о каждом окне и закладке Kaspersky Mobile Security: перечень и описание параметров и список решаемых задач.

## Документация

Руководство пользователя содержит описание интерфейса программы, предложены способы решения типовых задач пользователя при работе с программой.

## ОБСУЖДЕНИЕ ПРОГРАММ «ЛАБОРАТОРИИ КАСПЕРСКОГО» НА ФОРУМЕ

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме (<http://forum.kaspersky.com>).

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

## ОБРАЩЕНИЕ В ДЕПАРТАМЕНТ ПРОДАЖ

Если у вас возникли вопросы по выбору, приобретению или продлению срока использования программы, вы можете связаться с нашими специалистами из Департамента продаж одним из следующих способов:

- Позвонив по телефонам нашего центрального офиса в Москве (<http://www.kaspersky.ru/contacts>).
- Отправив письмо с вопросом по электронному адресу [sales@kaspersky.com](mailto:sales@kaspersky.com).

Обслуживание осуществляется на русском и английском языках.

## ОБРАЩЕНИЕ В ОТДЕЛ ЛОКАЛИЗАЦИИ И РАЗРАБОТКИ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ

Для обращения в Группу разработки документации требуется отправить письмо по адресу [docfeedback@kaspersky.com](mailto:docfeedback@kaspersky.com). В качестве темы письма нужно указать «Kaspersky Help Feedback: Kaspersky Mobile Security».

# KASPERSKY MOBILE SECURITY

Kaspersky Mobile Security обеспечивает защиту ваших данных от вирусов и других вредоносных программ и предотвращает кражу ваших персональных данных (фишинг) во время работы в сети. Kaspersky Mobile Security скрывает ваши конфиденциальные контакты и связанную с ними информацию, а также блокирует нежелательные входящие вызовы и SMS. В случае кражи или потери вашего устройства Kaspersky Mobile Security позволяет найти устройство и защитить вашу информацию на нем при помощи специальных SMS-команд или веб-портала <https://anti-theft.kaspersky.com>.

Kaspersky Mobile Security включает следующие компоненты:

- **Сканер (Антивирус Premium).**

Сканер (Антивирус Premium) защищает ваше устройство от вирусов и других вредоносных программ.

С помощью Сканера вы можете проверять на наличие угроз все устройство, только установленные программы или выбранную папку, а также обновлять антивирусные базы, обеспечивающие актуальную защиту ваших данных.

Антивирус (Premium) защищает ваше устройство в режиме реального времени, а также проверяет новые установленные программы до их первого запуска, используя антивирусные базы и облачный онлайн-сервис Kaspersky Security Network. Также Антивирус (Premium) позволяет автоматически проверять все устройство и обновлять антивирусные базы.

- **Личные контакты (Premium).**

Личные контакты позволяют временно скрывать ваши конфиденциальные контакты, а также историю разговоров и SMS-переписку с этими контактами. Личные контакты позволяют скрывать контакты и связанную с ними информацию в параметрах программы или дистанционно при помощи специальной SMS-команды.

- **Анти-Вор и веб-портал <https://anti-theft.kaspersky.com>.**

Когда устройство потеряно или украдено, Анти-Вор защищает информацию на устройстве от попадания в чужие руки, а также помогает найти его.

Анти-Вор позволяет вам дистанционно включить громкую сирену на устройстве, заблокировать устройство, определить его местонахождение, удалить хранящуюся на нем информацию или получить фотографии человека, который сейчас использует ваше устройство. Анти-Вор позволяет дистанционно запускать функции на устройстве при помощи специальных SMS-команд или веб-портала <https://anti-theft.kaspersky.com>. При замене SIM-карты (или включении устройства без нее) Анти-Вор позволяет получить новый номер телефона по SMS или электронной почте, а также заблокировать устройство.

- **Фильтр вызовов и SMS.**

Фильтр вызовов и SMS блокирует нежелательные входящие вызовы и SMS.

- **Веб-Фильтр (Premium) и SMS Анти-Фишинг (Premium).**

Веб-Фильтр блокирует вредоносные веб-сайты, цель которых – распространить вредоносный код, а также поддельные (фишинговые) веб-сайты, цель которых – украсть ваши конфиденциальные данные, такие как пароли от онлайн-банков, онлайн-аукционов или систем оплаты, и получить доступ к вашим финансовым счетам.

SMS Анти-Фишинг блокирует ссылки в SMS на вредоносные и поддельные веб-сайты.

**В ЭТОМ РАЗДЕЛЕ**

Что нового.....	<a href="#">11</a>
Аппаратные и программные требования.....	<a href="#">11</a>
Комплект поставки.....	<a href="#">12</a>
Сервис для пользователей.....	<a href="#">12</a>

**ЧТО НОВОГО**

В Kaspersky Mobile Security появились следующие новые возможности:

- Улучшена работа Антивируса: проверка устройства выполняется быстрее за счет обновленного механизма сканирования. Также добавлена быстрая проверка, которая позволяет проверять на наличие угроз только установленные программы.
- Добавлена новая функция SMS Анти-Фишинг. SMS Анти-Фишинг предотвращает кражу ваших персональных данных, проверяя ссылки в SMS на вредоносные и поддельные веб-сайты.
- Добавлена новая функция Сирена. С помощью этой функции в случае кражи или потери вашего устройства вы сможете заблокировать устройство и включить на нем сирену при помощи веб-портала <https://anti-theft.kaspersky.com> или SMS-команды `alarm: <код>` (где <код> – это секретный код Kaspersky Mobile Security на вашем устройстве).
- Объединены функции Блокирование и Поиск. В случае кражи или потери вашего устройства вы можете заблокировать устройство и одновременно получить координаты его местоположения при помощи веб-портала <https://anti-theft.kaspersky.com> или SMS-команды `find: <код>` (где <код> – это секретный код Kaspersky Mobile Security на вашем устройстве).
- Улучшена функциональность Тайного фото: в случае кражи или потери вашего устройства вы сможете заблокировать устройство и одновременно получить фотографии человека, который сейчас использует ваше устройство, при помощи веб-портала <https://anti-theft.kaspersky.com>.
- Улучшена стабильность программы: исправлены ошибки, приводящие к сбою в работе программы.
- Изменена схема лицензирования программы: после установки программы автоматически доступна бесплатная версия. Чтобы оценить все функции программы в течение ознакомительного периода, вы можете перейти на пробную версию программы. Чтобы получить доступ ко всем функциям программы, вы можете приобрести лицензию и перейти на коммерческую версию программы.

Включение Сирены через веб-портал будет доступно позже официального выпуска новой версии Kaspersky Mobile Security.

Запуск Блокирования и Поиска одной командой через веб-портал будет доступен позже официального выпуска новой версии Kaspersky Mobile Security. Через необновленный веб-портал вы можете запустить Блокирование и Поиск двумя командами.

**АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ**

Kaspersky Mobile Security устанавливается на устройства, работающие под управлением операционной системы Android™ 2.2 – 4.2.

Программа работает на устройствах с разрешением экрана от 320x480 пикселей.

## КОМПЛЕКТ ПОСТАВКИ

Вы можете приобрести программу одним из следующих способов:

- **В коробке.** Распространяется через магазины наших партнеров.
- **Через интернет-магазин.** Распространяется через интернет-магазины «Лаборатории Касперского» (например, <http://www.kaspersky.ru>, раздел **Интернет-магазин**) или компаний-партнеров.

Если вы приобретаете программу в коробке, в комплект поставки входят следующие компоненты:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программы и файлы документации к программе;
- краткое руководство пользователя, содержащее код активации программы;
- Лицензионное соглашение, в котором указано, на каких условиях вы можете пользоваться программой.

Состав комплекта поставки может быть различным в зависимости от региона, в котором распространяется программа.

Если вы приобретаете Kaspersky Mobile Security через интернет-магазин, вы копируете программу с сайта интернет-магазина. Информация, необходимая для активации программы, высылается вам по электронной почте после оплаты.

За подробной информацией о способах приобретения и комплекте поставки вы можете обратиться в Департамент продаж по адресу [sales@kaspersky.com](mailto:sales@kaspersky.com).

## СЕРВИС ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

Приобретая лицензию на использование программы, в течение срока действия лицензии вы можете получать следующие услуги:

- обновление баз и предоставление новых версий программы;
- консультации по телефону и электронной почте по вопросам, связанным с установкой, настройкой и использованием программы;
- оповещение о выходе новых программ «Лаборатории Касперского», а также информацию о появлении новых вирусов и вирусных эпидемиях. Для использования этой услуги требуется подписаться на рассылку новостей ЗАО «Лаборатория Касперского» на веб-сайте Службы технической поддержки.

Консультации по работе операционных систем, стороннего программного обеспечения и технологиям не проводятся.

# ИНТЕРФЕЙС ПРОГРАММЫ

Этот раздел содержит информацию об основных элементах графического интерфейса программы: значке программы, главном окне, окне настройки, виджете и окнах уведомлений.

## В ЭТОМ РАЗДЕЛЕ

---

Значок в области уведомлений.....	<a href="#">13</a>
Главное окно Kaspersky Mobile Security.....	<a href="#">13</a>
Виджет для главного экрана устройства.....	<a href="#">15</a>
Уведомления.....	<a href="#">15</a>

## ЗНАЧОК В ОБЛАСТИ УВЕДОМЛЕНИЙ

После первоначальной настройки программы Kaspersky Mobile Security ее значок появляется в строке состояния.

Значок выполняет следующие функции:

- служит индикатором работы программы;
- обеспечивает доступ к главному окну программы.

### Индикация работы программы

Значок служит индикатором работы программы. В коммерческой версии он отражает состояние защиты вашего устройства:



(цветной значок) – защита работает;



(черно-белый значок) – защита отключена;



– антивирусные базы устарели.

В бесплатной версии программы значок не отражает состояние защиты устройства.

### Доступ к окнам программы

С помощью значка программы из панели уведомлений вы можете открыть главное окно программы.

## ГЛАВНОЕ ОКНО KASPERSKY MOBILE SECURITY

В главном окне программы отображаются элементы интерфейса, предоставляющие доступ к основным функциям программы.

В главном окне отображаются блоки, соответствующие компонентам программы. В коммерческой версии программы отображаются блоки **Антивирус**, **Личные контакты**, **Анти-Вор**, **Фильтр вызовов** и **SMS**, **Веб-**

**Фильтр.** В бесплатной версии программы отображаются блоки **Сканер**, **Анти-Вор**, **Фильтр вызовов и SMS** и **SMS**. Также в главном окне отображается блок **Дополнительно**, в котором сгруппированы дополнительные возможности программы (см. рис. ниже).

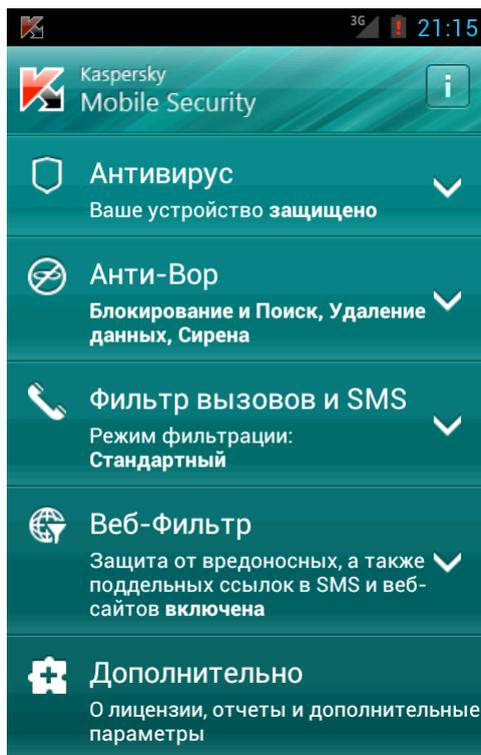


Рисунок 1. Главное окно в коммерческой версии программы

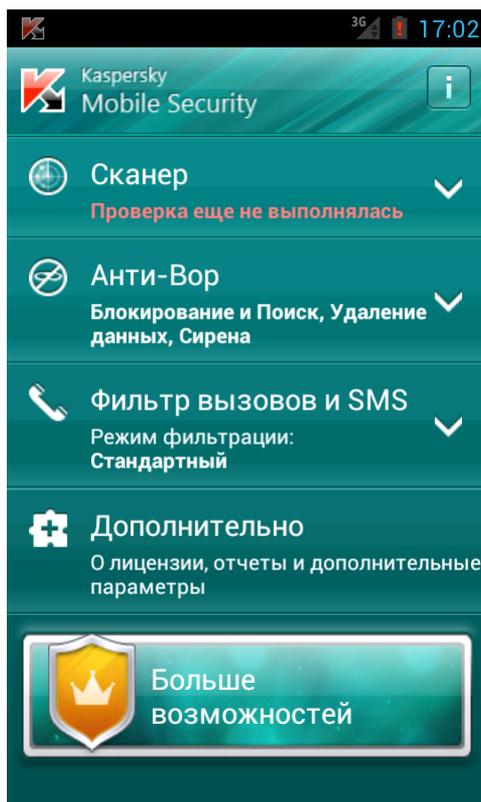


Рисунок 2. Главное окно в бесплатной версии программы

Блок, соответствующий компоненту программы, может быть свернут или развернут.

На свернутом блоке отображается информация о статусе компонента программы.

Развернутый блок позволяет перейти к основным функциям компонента программы (например, для блока **Антивирус** это выполнение задач проверки на вирусы, обновление баз и версий программы) или к настройке параметров этого компонента программы.



Также вы можете воспользоваться кнопкой (Справка), по которой открывается контекстная справка Kaspersky Mobile Security.

Вы можете открыть главное окно программы одним из следующих способов:

- нажав на значок программы в панели уведомлений;
- нажав на виджет программы.

## ВИДЖЕТ ДЛЯ ГЛАВНОГО ЭКРАНА УСТРОЙСТВА

При использовании Kaspersky Mobile Security вам доступен виджет главного экрана (см. рис. ниже).



Рисунок 3. Виджет главного экрана

Виджет используется для перехода к главному окну программы.

В коммерческой версии программы цвет виджета главного экрана сообщает о состоянии защиты вашего устройства. Также в коммерческой версии программы цвет виджета может сообщать о скрывании конфиденциальных контактов и связанной с ними информации, если это разрешено в настройках виджета.

Представлена следующая цветовая индикация:

- зеленый цвет щита означает, что защита включена;
- серый цвет щита означает, что защита отключена;
- зеленый цвет фона означает, что программа скрывает конфиденциальные контакты и связанную с ними информацию;
- серый цвет фона означает, что программа отображает конфиденциальные контакты и связанную с ними информацию.

В бесплатной версии программы цвет виджета не сигнализирует о состоянии защиты устройства.

## УВЕДОМЛЕНИЯ

Kaspersky Mobile Security уведомляет вас о значимых событиях, происходящих в процессе ее работы, с помощью *окон уведомлений* и *всплывающих уведомлений*, которые появляются в строке состояния.

*Окна уведомлений* Kaspersky Mobile Security выводит на экран в тех случаях, когда возможны различные варианты действий в связи с событием. Например, при обнаружении вредоносного объекта, когда программе не удалось его вылечить, вы можете удалить объект, пропустить его или открыть справку, чтобы узнать о возможных действиях с вредоносным файлом (см. рис. ниже). Программа предложит вам выбрать действие из числа возможных. Окно уведомления исчезнет с экрана только после того, как вы выберете одно из предложенных действий.

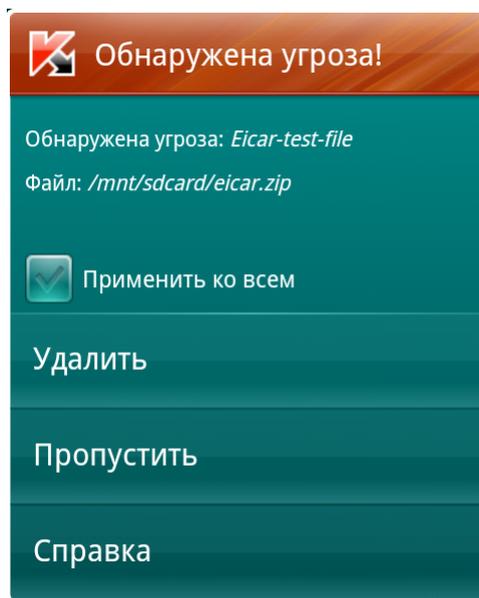


Рисунок 4. Всплывающее уведомление

*Всплывающие уведомления* Kaspersky Mobile Security показывает в строке состояния, чтобы проинформировать о событиях, не требующих от вас выбора действия (см. рис. ниже). В дальнейшем вы можете посмотреть уведомления в панели уведомлений вашего устройства.



Рисунок 5. Всплывающее уведомление

В зависимости от степени важности события с точки зрения безопасности устройства, уведомления делятся на три типа:

- **Критические** – информируют о событиях, имеющих первостепенную важность для обеспечения безопасности устройства (например, об обнаружении вредоносного файла).
- **Важные** – информируют о событиях, потенциально важных для обеспечения безопасности устройства (например, о запуске проверки или обновления).
- **Информационные** – информируют о событиях, не имеющих первостепенной важности для обеспечения безопасности устройства.

# ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

Этот раздел содержит информацию об основных понятиях, связанных с активацией программы. Из этого раздела вы узнаете о назначении Лицензионного соглашения, типах лицензии, способах активации программы, а также о продлении срока действия лицензии.

## В ЭТОМ РАЗДЕЛЕ

О Лицензионном соглашении .....	<a href="#">17</a>
О лицензии.....	<a href="#">17</a>
О коде активации.....	<a href="#">18</a>

## О ЛИЦЕНЗИОННОМ СОГЛАШЕНИИ

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. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы или не использовать программу.

## О ЛИЦЕНЗИИ

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

Лицензия включает в себя право на получение следующих видов услуг:

- Использование программы на одном или нескольких устройствах.

Количество устройств, на которых вы можете использовать программу, определяется условиями Лицензионного соглашения.

- Обращение в Службу технической поддержки «Лаборатории Касперского».
- Получение прочих услуг, предоставляемых вам «Лабораторией Касперского» или ее партнерами в течение срока действия лицензии. (см. раздел «Сервис для пользователей» на стр. [12](#))

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- **Бесплатная лицензия.** По бесплатной лицензии доступна бесплатная версия, которая позволяет использовать ограниченную функциональность Kaspersky Mobile Security в течение неограниченного периода времени. Ограничения бесплатной версии программы указаны в Лицензионном соглашении. Бесплатная версия доступна сразу после установки программы. С бесплатной версии вы можете перейти на пробную версию или коммерческую версию программы.
- **Пробная лицензия.** Пробная лицензия распространяется безвозмездно. По пробной лицензии активируется пробная версия, которая позволяет использовать все функции программы в течение ознакомительного периода.

С пробной версии вы можете перейти на коммерческую версию или бесплатную версию программы. Если ознакомительный период истек, программа автоматически переключится на бесплатную версию.

- **Коммерческая лицензия.** Коммерческая лицензия предоставляется после приобретения программы. По коммерческой лицензии вы можете активировать коммерческую версию, которая предоставляет доступ ко всем функциям программы. Коммерческая лицензия имеет ограниченный срок действия.

Когда срок действия коммерческой лицензии истекает, вы можете продолжить использование программы. Для этого вы можете продлить срок действия коммерческой лицензии или переключиться на бесплатную версию программы. Для продления срока действия лицензии вы можете ввести новый код активации, полученный при покупке программы, либо приобрести новую лицензию в интернет-магазине.

Когда срок действия коммерческой лицензии истек, программа автоматически переключится на бесплатную версию.

## О КОДЕ АКТИВАЦИИ

*Код активации* – это код, который вы получаете, приобретая коммерческую лицензию на использование Kaspersky Mobile Security. Этот код необходим для активации программы.

Код активации представляет собой уникальную последовательность из двадцати латинских букв и цифр в формате xxxxx-xxxxx-xxxxx-xxxxx.

В зависимости от способа приобретения программы возможны следующие варианты получения кода активации:

- Если вы приобрели коробочную версию Kaspersky Mobile Security, код активации указан в документации или на коробке, в которой находится установочный компакт-диск.
- Если вы приобрели Kaspersky Mobile Security в интернет-магазине, код активации высылается по адресу электронной почты, указанному вами при заказе.

Отсчет срока действия лицензии начинается с даты активации программы. Если вы приобрели лицензию, допускающую использование Kaspersky Mobile Security на нескольких устройствах, то отсчет срока действия лицензии начинается с даты первого применения кода активации.

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

# ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ

Kaspersky Mobile Security запускается при старте операционной системы и защищает ваше устройство в течение всего сеанса работы.

Вы можете завершить работу с программой, удалив Kaspersky Mobile Security или отключив все компоненты программы.

«Лаборатория Касперского» не рекомендует отключать все компоненты Kaspersky Mobile Security, поскольку в этом случае безопасность вашего устройства и ваших личных данных окажется под угрозой.

# РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ

Этот раздел содержит пошаговые инструкции для выполнения основных задач пользователя, которые решает программа.

## В ЭТОМ РАЗДЕЛЕ

---

Как активировать коммерческую версию программы .....	<a href="#">21</a>
Как приобрести лицензию или продлить срок ее действия .....	<a href="#">21</a>
Как посмотреть информацию о лицензии, узнать срок ее действия .....	<a href="#">22</a>
Как проверить всю файловую систему устройства на вирусы.....	<a href="#">22</a>
Как проверить на вирусы установленные программы, папку или файл.....	<a href="#">22</a>
Как настроить автоматический запуск проверки всего устройства на вирусы .....	<a href="#">23</a>
Как обновить антивирусные базы и версию программы .....	<a href="#">23</a>
Как настроить автоматическое обновление антивирусных баз и версий программы по расписанию.....	<a href="#">24</a>
Как скрывать контакты и связанную с ними информацию .....	<a href="#">24</a>
Как дистанционно с другого устройства скрыть контакты и связанную с ними информацию .....	<a href="#">25</a>
Что такое Kaspersky Account .....	<a href="#">26</a>
Как добавить устройство в мою учетную запись на веб-портале .....	<a href="#">26</a>
Что делать, если устройство потеряно или украдено .....	<a href="#">26</a>
Как отправить SMS-команды с другого устройства, на котором установлена Kaspersky Mobile Security.....	<a href="#">28</a>
Как разрешить или запретить дистанционно запускать функции Анти-Вора на устройстве .....	<a href="#">28</a>
Как при замене SIM-карты узнать новый номер телефона и заблокировать устройство .....	<a href="#">30</a>
Как дистанционно заблокировать устройство и узнать его местоположение.....	<a href="#">30</a>
Как дистанционно включить сирену на устройстве .....	<a href="#">31</a>
Как удалить персональные данные с устройства или полностью отформатировать его .....	<a href="#">32</a>
Как получить фотографии человека, который сейчас использует ваше устройство .....	<a href="#">33</a>
Как избавиться от нежелательных вызовов и SMS .....	<a href="#">34</a>
Как защитить персональные данные от кражи в сети .....	<a href="#">35</a>
Как посмотреть отчеты о работе программы .....	<a href="#">36</a>
Как изменить секретный код программы .....	<a href="#">36</a>
Как восстановить секретный код программы .....	<a href="#">36</a>

## КАК АКТИВИРОВАТЬ КОММЕРЧЕСКУЮ ВЕРСИЮ ПРОГРАММЫ

Вы можете использовать одну из следующих версий программы: бесплатную, пробную или коммерческую (см. раздел «О лицензии» на стр. [17](#)).

С бесплатной или пробной версии вы можете перейти на коммерческую версию программы, предоставляющую доступ ко всем функциям программы. Для этого ее нужно активировать.

*Активация* – это процедура введения в действие лицензии на использование полнофункциональной версии программы в течение определенного срока.

Чтобы активировать коммерческую версию, вам нужно ввести код активации (см. раздел «О коде активации» на стр. [18](#)), который вы получили при приобретении программы, либо приобрести лицензию в интернет-магазине.

Вы можете активировать коммерческую версию из мастера первоначальной настройки программы либо из меню программы.

Для активации программы нужно активное интернет-соединение.

➔ *Чтобы активировать коммерческую версию программы с помощью кода активации из мастера первоначальной настройки программы, выполните следующие действия:*

1. На последнем шаге мастера первоначальной настройки нажмите **У меня есть код активации**.
2. Введите код активации в открывшемся окне и нажмите **Активировать**.

Программа отправит запрос на активацию на сервер активации «Лаборатории Касперского». При успешном выполнении запроса на активацию программа уведомит вас об этом и покажет информацию о лицензии.

➔ *Чтобы активировать коммерческую версию программы с помощью кода активации в меню программы, выполните следующие действия:*

1. В главном окне Kaspersky Mobile Security нажмите **Дополнительно > Лицензирование > Ввод кода активации**.
2. Введите код активации в открывшемся окне и нажмите **Активировать**.

Программа отправит запрос на активацию на сервер активации «Лаборатории Касперского». При успешном выполнении запроса на активацию программа уведомит вас об этом и покажет информацию о лицензии.

## КАК ПРИОБРЕСТИ ЛИЦЕНЗИЮ ИЛИ ПРОДЛИТЬ СРОК ЕЕ ДЕЙСТВИЯ

Если вы решили использовать полную функциональность Kaspersky Mobile Security, вы можете приобрести лицензию в интернет-магазине. При приобретении лицензии вы получите код активации, с помощью которого вам нужно активировать коммерческую версию программы (см. раздел «Как активировать коммерческую версию программы» на стр. [21](#)).

Когда срок действия коммерческой лицензии подходит к концу, вы можете его продлить. Для этого вы можете ввести новый код активации (см. раздел «О коде активации» на стр. [18](#)), полученный при приобретении лицензии, либо приобрести новую лицензию в интернет-магазине.

Когда срок действия коммерческой лицензии истек, программа автоматически переходит на бесплатную версию.

➤ *Чтобы приобрести лицензию в интернет-магазине или продлить срок действия лицензии, выполните следующие действия:*

1. В главном окне Kaspersky Mobile Security нажмите **Дополнительно > Лицензирование**.
2. Выполните одно из действий в зависимости от задачи:
  - Чтобы приобрести новую лицензию, выберите **Приобретение лицензии**, затем нажмите **Открыть**.  
Откроется веб-страница интернет-магазина, где вы можете приобрести новую лицензию.
  - Чтобы ввести новый код активации, выберите **Ввод кода активации**, затем введите новый код активации, полученный при приобретении лицензии.

## КАК ПОСМОТРЕТЬ ИНФОРМАЦИЮ О ЛИЦЕНЗИИ, УЗНАТЬ СРОК ЕЕ ДЕЙСТВИЯ

Вы можете посмотреть ключ, срок действия лицензии, тип и другую дополнительную информацию о лицензии.

*Информация доступна для просмотра, если активирована пробная или коммерческая версия программы.*

➤ *Чтобы проверить срок действия лицензии и посмотреть информацию о лицензии, выполните следующее:*

В главном окне Kaspersky Mobile Security нажмите **Дополнительно > Лицензирование > Подробнее о лицензии**.

## КАК ПРОВЕРИТЬ ВСЮ ФАЙЛОВУЮ СИСТЕМУ УСТРОЙСТВА НА ВИРУСЫ

Полная проверка всего устройства на наличие вирусов и других вредоносных программ помогает защитить ваши личные данные и деньги, а также обнаружить и устранить угрозы на вашем устройстве (как в установленных программах, так и в дистрибутивах).

Большинство вредоносных программ угрожают именно личным данным пользователя на устройстве: они собирают личные данные владельца устройства, всю имеющуюся информацию об устройстве (например, GPS-координаты, почту) и отправляют ее злоумышленникам.

Рекомендуется проверить всю файловую систему устройства на вирусы хотя бы один раз после установки программы, чтобы убедиться в безопасности личных данных.

➤ *Чтобы проверить всю файловую систему устройства на вирусы и другие вредоносные программы, выполните следующее:*

В главном окне Kaspersky Mobile Security нажмите **Сканер (Антивирус Premium) > Проверка > Полная проверка**.

## КАК ПРОВЕРИТЬ НА ВИРУСЫ УСТАНОВЛЕННЫЕ ПРОГРАММЫ, ПАПКУ ИЛИ ФАЙЛ

Вы можете проверить папку, файл или только установленные программы.

Большинство угроз скрыто в программах. Чтобы защитить ваши данные, «Лаборатория Касперского» рекомендует запускать быструю проверку (проверку установленных программ) после установки новых программ.

Проверка файла позволяет вам убедиться в его безопасности, например, когда файл был загружен из интернета.

► *Чтобы проверить только установленные программы, выполните следующее:*

В главном окне Kaspersky Mobile Security нажмите **Сканер (Антивирус Premium) > Проверка > Быстрая проверка**.

► *Чтобы проверить папку или файл, выполните следующие действия:*

1. В главном окне Kaspersky Mobile Security нажмите **Сканер (Антивирус Premium) > Проверка > Проверка папки**.
2. Выберите папку или файл для проверки.

## КАК НАСТРОИТЬ АВТОМАТИЧЕСКИЙ ЗАПУСК ПРОВЕРКИ ВСЕГО УСТРОЙСТВА НА ВИРУСЫ

Вы можете настроить автоматический запуск полной проверки устройства и создать расписание ее запуска: выбрать периодичность, день и время запуска, если это необходимо. Программа будет автоматически проверять всю файловую систему устройства по сформированному расписанию.

Для автоматического запуска полной проверки требуется, чтобы устройство в это время было включено.

► *Чтобы настроить автоматический запуск проверки по расписанию, выполните следующие действия:*

1. В главном окне Kaspersky Mobile Security нажмите **Сканер (Антивирус Premium) > Настройка > Параметры проверки**.
2. Выберите периодичность запуска проверки. Для этого выберите значение для параметра **Расписание**.
3. Выберите день и время запуска проверки. Для этого выберите значения для параметров **День запуска** и **Время запуска**.

## КАК ОБНОВИТЬ АНТИВИРУСНЫЕ БАЗЫ И ВЕРСИЮ ПРОГРАММЫ

Kaspersky Mobile Security при поиске вредоносных программ использует антивирусные базы. Антивирусные базы программы содержат описание известных «Лаборатории Касперского» в настоящий момент вредоносных программ и способов их обезвреживания, а также описание других вредоносных объектов. Поэтому настоятельно рекомендуется регулярно обновлять антивирусные базы. Если с момента последнего обновления прошло более 15-ти дней, антивирусные базы программы считаются устаревшими. В этом случае надежность защиты снижается.

Помимо антивирусных баз Kaspersky Mobile Security позволяет обновлять версии программы. Обновления версии программы устраняют уязвимости Kaspersky Mobile Security, добавляют новые функции или улучшают существующие.

Чтобы обновить антивирусные базы и версию программы, требуется соединение с интернетом.

Если вы загрузили Kaspersky Mobile Security из Google Play, то программа обновляет только антивирусные базы. Версия программы обновляется через Google Play.

➤ Чтобы обновить антивирусные базы и версию программы, выполните следующее:

В главном окне Kaspersky Mobile Security нажмите **Сканер (Антивирус Premium) > Обновление**.

## КАК НАСТРОИТЬ АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ АНТИВИРУСНЫХ БАЗ И ВЕРСИЙ ПРОГРАММЫ ПО РАСПИСАНИЮ

Вы можете настроить автоматический запуск обновления антивирусных баз и версии программы (далее «обновление»). Для этого вы можете создать расписание его запуска: выбрать периодичность, день и время запуска, если это необходимо. Программа будет автоматически обновлять антивирусные базы и версии программы по сформированному расписанию.

Автоматическое обновление доступно только в коммерческой версии Kaspersky Mobile Security.

Для обновления требуется соединение с интернетом.

Для автоматического обновления в выбранное время требуется, чтобы устройство в это время было включено.

➤ Чтобы настроить автоматический запуск обновления по расписанию, выполните следующие действия:

1. В главном окне Kaspersky Mobile Security нажмите **Антивирус > Настройка > Параметры обновления**.
2. Выберите периодичность запуска обновления. Для этого установите значение для параметра **Расписание**.
3. Выберите день и время запуска обновления. Для этого установите значение для параметров **День запуска** и **Время запуска**.

## КАК СКРЫВАТЬ КОНТАКТЫ И СВЯЗАННУЮ С НИМИ ИНФОРМАЦИЮ

Вы можете временно скрыть важные контакты, а также SMS-переписку и историю разговоров с этими контактами. Для этого вы можете использовать функцию Личные контакты.

Личные контакты доступны только в коммерческой версии Kaspersky Mobile Security.

Для конфиденциальных контактов программа позволяет скрывать следующую информацию:

- записи в Kontakтах;
- прочитанные входящие SMS, переданные и черновики SMS;
- записи в журнале вызовов;
- входящие вызовы и уведомления о новых SMS.

Вы можете включить скрытие информации на устройстве в параметрах программы или дистанционно с помощью SMS-команды, отправленной с другого мобильного устройства (см. раздел «Как дистанционно с другого устройства скрыть контакты и связанную с ними информацию» на стр. 25). Вы можете отправить стандартное SMS со специальным текстом или отправить SMS из Kaspersky Mobile Security, если программа установлена на другом устройстве.

На своем устройстве вы можете запретить или разрешить дистанционный запуск скрытия информации. Если дистанционный запуск скрытия информации запрещен, то эту функцию невозможно запустить дистанционно с помощью SMS-команды.

Вы можете отключить скрытие информации только в программе, установленной на вашем устройстве.

➡ *Чтобы скрывать контакты и связанную с ними информацию, выполните следующие действия:*

1. Создайте список скрываемых контактов, если он еще не создан. В списке хранятся контакты, для которых вы хотите скрывать информацию. В главном окне Kaspersky Mobile Security нажмите **Личные контакты > Скрываемые контакты > Добавить**. Чтобы импортировать контакт из записной книги, выберите **Контакт**. Чтобы добавить номер, выберите **Номер телефона**.
2. Если требуется, выберите информацию, которую нужно скрывать для выбранных контактов, а также настройте дополнительные параметры Личных контактов. Для этого вернитесь в главное окно Kaspersky Mobile Security > **Личные контакты** и нажмите **Настройка**.
3. Скройте контакты и связанную с ними информацию. Для этого выполните одно из следующих действий:
  - Вернитесь в главное окно Kaspersky Mobile Security > **Личные контакты** и установите переключатель **Скрыть информацию** в состояние **включено**.
  - Дистанционно с другого устройства отправьте на ваше устройство специальную SMS-команду (см. раздел «Как дистанционно с другого устройства скрыть контакты и связанную с ними информацию» на стр. 25).

## КАК ДИСТАНЦИОННО С ДРУГОГО УСТРОЙСТВА СКРЫТЬ КОНТАКТЫ И СВЯЗАННУЮ С НИМИ ИНФОРМАЦИЮ

При необходимости вы можете дистанционно скрыть контакты и связанную с ними информацию. Для этого с другого устройства вам нужно отправить специальную SMS-команду.

Скрытие контактов и связанной с ними информации возможно, если на вашем устройстве активирована коммерческая версия Kaspersky Mobile Security.

Вы можете отправить стандартное SMS со специальным текстом или отправить SMS из Kaspersky Mobile Security, если программа установлена на другом устройстве.

Предварительно на вашем устройстве вы можете запретить или разрешить дистанционный запуск скрытия информации.

Дистанционный запуск скрытия информации возможен, если выполнены следующие условия: активирована коммерческая версия программы, сигнал сотовой связи есть на устройстве и дистанционный запуск этой функции разрешен на устройстве.

- *Чтобы дистанционно скрыть информацию на своем устройстве, на другом устройстве выполните одно из следующих действий:*
  - Сформируйте и отправьте команду на свое устройство из Kaspersky Mobile Security с помощью функции отправки SMS-команды, если программа установлена на другом устройстве.
  - Создайте и отправьте на ваше устройство SMS со специальным текстом `hide:<код>` (где `<код>` – это секретный код Kaspersky Mobile Security на вашем устройстве).

Отправка SMS-команды на ваше устройство оплачивается согласно тарифу оператора сотовой связи, используемого на другом мобильном устройстве.

## ЧТО ТАКОЕ KASPERSKY ACCOUNT

Учетная запись нужна вам для того, чтобы при помощи веб-портала <https://anti-theft.kaspersky.com> дистанционно включить сирену на устройстве, заблокировать устройство, узнать его местоположение на карте, удалить с него данные или незаметно сделать фотографии человека, который пользуется вашим устройством в данный момент. Также через веб-портал вы можете восстановить забытый секретный код от Kaspersky Mobile Security.

Kaspersky Account – это единая учетная запись для доступа ко всем сервисам «Лаборатории Касперского». Если вы зарегистрированы в таких сервисах, как Личный кабинет, или если у вас есть учетная запись для веб-портала <https://anti-theft.kaspersky.com>, то это значит, что у вас есть Kaspersky Account.

Вы указываете учетную запись при первоначальной настройке программы. В качестве имени пользователя используется ваш адрес электронной почты. Если при входе на веб-портал вы забыли пароль от учетной записи, вы можете его восстановить.

## КАК ДОБАВИТЬ УСТРОЙСТВО В МОЮ УЧЕТНУЮ ЗАПИСЬ НА ВЕБ-ПОРТАЛЕ

Вы можете управлять несколькими устройствами одновременно через вашу учетную запись на веб-портале <https://anti-theft.kaspersky.com>.

Чтобы добавить устройство к вашей учетной записи, во время первоначальной настройки Kaspersky Mobile Security на новом устройстве введите данные вашей учетной записи.

Новое устройство будет автоматически привязано к вашей учетной записи. После входа на веб-портал появится новая закладка с именем устройства.

## ЧТО ДЕЛАТЬ, ЕСЛИ УСТРОЙСТВО ПОТЕРЯНО ИЛИ УКРАДЕНО

В случае кражи или потери устройства вы можете дистанционно скрыть контакты и связанную с ними информацию, а также запустить функции Анти-Вора: включить сирену, заблокировать свое устройство, удалить хранящуюся на нем информацию, получить его местоположение на карте или незаметно сделать фотографии человека, который пользуется вашим устройством в данный момент.

Вы можете дистанционно запустить функции Анти-Вора через веб-портал <https://anti-theft.kaspersky.com> или при помощи специальных SMS-команд, отправленных с любого устройства.

Вы можете дистанционно скрыть контакты и связанную с ними информацию только при помощи специальной SMS-команды.

Скрытие контактов и связанной с ними информации возможно, если на вашем устройстве активирована коммерческая версия Kaspersky Mobile Security.

Вы можете отправить команду сделать фотографии человека, который сейчас использует ваше устройство, только через веб-портал <https://anti-theft.kaspersky.com>. Отправка такой команды по SMS не поддерживается.

Отправка SMS оплачивается согласно тарифу оператора сотовой связи на том устройстве, с которого отправляется SMS-команда.

Дистанционный запуск функции Анти-Вора и скрытия информации возможен, если выполнены следующие условия: программа Kaspersky Mobile Security установлена в качестве администратора устройства, сигнал сотовой связи есть на устройстве и дистанционный запуск этой функции разрешен на устройстве.

➤ Чтобы дистанционно через <https://anti-theft.kaspersky.com> запустить функции Анти-Вора, 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, 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 нужно дистанционно запустить функции Анти-Вора.
4. Выберите в блоках сверху нужное действие для устройства.

➤ Чтобы дистанционно при помощи SMS-команд скрыть информацию и запустить функции Анти-Вора, выполните одно из следующих действий:

- Сформируйте и отправьте команду на свое устройство из Kaspersky Mobile Security с помощью функции отправки SMS-команды, если программа установлена на другом устройстве (см. раздел «Как отправить SMS-команды с другого устройства, на котором установлена Kaspersky Mobile Security» на стр. 28).

При формировании SMS-команды используйте секретный код Kaspersky Mobile Security, установленной на вашем устройстве.

- Отправьте SMS на ваше устройство со следующим специальным текстом:
  - `hide: <код>` – для скрытия конфиденциальных контактов и связанной с ними информации;
  - `alarm: <код>` – для включения сирены и блокирования устройства;
  - `find: <код>` – для блокирования устройства и определения его местоположения;
  - `wipe: <код>` – для удаления персональных данных и данных на карте памяти;
  - `fullreset: <код>` – для удаления всех данных с устройства и возврата устройства к заводским настройкам.

После выполнения команды удалить все данные программа Kaspersky Mobile Security будет удалена и устройство не сможет получать последующие дистанционные команды.

<Код> – это секретный код Kaspersky Mobile Security, установленной на вашем устройстве.

## КАК ОТПРАВИТЬ SMS-КОМАНДЫ С ДРУГОГО УСТРОЙСТВА, НА КОТОРОМ УСТАНОВЛЕНА KASPERSKY MOBILE SECURITY

В случае кражи или потери вашего устройства вы можете дистанционно запустить функции Анти-Вора или скрыть конфиденциальную информацию на устройстве. Для этого нужно отправить на ваше устройство специальные команды либо через веб-портал <https://anti-theft.kaspersky.com>, либо по SMS.

С другого мобильного устройства вы можете отправить на ваше устройство стандартное SMS со специальным текстом (см. раздел «Что делать, если устройство потеряно или украдено» на стр. 26). Если на другом мобильном устройстве установлена Kaspersky Mobile Security, вы можете отправить SMS-команду из программы. Для отправки SMS-команды требуется знать секретный код программы Kaspersky Mobile Security на вашем устройстве.

Отправка SMS-команды на ваше устройство оплачивается согласно тарифу оператора сотовой связи, используемого на другом мобильном устройстве.

➤ Чтобы дистанционно запустить функции Анти-Вора и скрыть информацию с устройства, на котором установлена программа Kaspersky Mobile Security, выполните следующие действия:

1. Откройте на другом устройстве программу Kaspersky Mobile Security.
2. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор** > **Отправка SMS-команд**.

В более ранних версиях программы путь к функции отправки SMS-команды отличается: главное окно Kaspersky Mobile Security > **Анти-Вор** > **Удаленное управление** или главное окно Kaspersky Mobile Security > **Дополнительно** > **Отправка SMS-команды**.

3. Нажмите **Отправить SMS-команду**, затем сформируйте и отправьте команду на ваше устройство. При формировании SMS-команды используйте секретный код Kaspersky Mobile Security, установленной на вашем устройстве.

## КАК РАЗРЕШИТЬ ИЛИ ЗАПРЕТИТЬ ДИСТАНЦИОННО ЗАПУСКАТЬ ФУНКЦИИ АНТИ-ВОРА НА УСТРОЙСТВЕ

В случае кражи или потери вашего устройства вы можете запускать функции Анти-Вора дистанционно с помощью специальных SMS-команд или через веб-портал <https://anti-theft.kaspersky.com>. Предварительно на устройстве вы можете запретить или разрешить дистанционно запускать функции Анти-Вора.

Если запуск функции Анти-Вора запрещен, то эту функцию невозможно запускать дистанционно.

Вы можете разрешить или запретить дистанционно включать сирену на устройстве, блокировать устройство, определять его местоположение, удалять данные с него, а также незаметно фотографировать человека, который сейчас пользуется вашим устройством.

➤ Чтобы разрешить дистанционное включение сирены и блокирование устройства, выполните следующие действия:

1. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор** > **Настройка**.
2. Установите флажок **Сирена**.

- *Чтобы запретить дистанционное включение сирены и блокирование устройства, выполните следующие действия:*
  1. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор > Настройка**.
  2. Снимите флажок **Сирена**.
- *Чтобы разрешить дистанционное блокирование своего устройства и определение его местоположения, выполните следующие действия:*
  1. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор > Настройка**.
  2. Установите флажок **Блокирование и Поиск**.
  3. Если требуется, в поле **Текст при блокировании** введите текст сообщения, которое будет отображаться на экране заблокированного устройства.
  4. Если требуется, в блоке **Способы получения нового телефона при смене SIM-карты и местоположения устройства** укажите адрес электронной почты, на который вы хотите получить местоположение вашего устройства.
- *Чтобы запретить дистанционное блокирование своего устройства и определение его местоположения, выполните следующие действия:*
  1. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор > Настройка**.
  2. Снимите флажок **Блокирование и Поиск**.
- *Чтобы разрешить дистанционное удаление данных со своего устройства, выполните следующие действия:*
  1. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор > Настройка**.
  2. Установите флажок **Удаление данных**, чтобы разрешить дистанционное удаление персональных данных (например, контактов, SMS-переписки или календаря) и данных на карте памяти.
  3. Установите флажок **Сброс к заводским настройкам**, чтобы разрешить дистанционное удаление всех данных, включая данные на карте памяти, и возврат устройства к заводским настройкам.
- *Чтобы запретить дистанционное удаление данных со своего устройства, выполните следующие действия:*
  1. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор > Настройка**.
  2. Снимите флажки **Удаление данных** и **Сброс к заводским настройкам**.
- *Чтобы разрешить дистанционное фотографирование с устройства, выполните следующее:*
  1. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор > Настройка**.
  2. Установите флажок **Тайное фото**.
- *Чтобы запретить дистанционное фотографирование с устройства, выполните следующее:*
  1. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор > Настройка**.
  2. Снимите флажок **Тайное фото**.

## КАК ПРИ ЗАМЕНЕ SIM-КАРТЫ УЗНАТЬ НОВЫЙ НОМЕР ТЕЛЕФОНА И ЗАБЛОКИРОВАТЬ УСТРОЙСТВО

В случае смены SIM-карты или включения устройства без нее, Анти-Вор позволяет заблокировать устройство и узнать новый номер телефона, чтобы дистанционно запустить другие функции Анти-Вора на устройстве.

Вы можете получить новый номер телефона по SMS или по электронной почте.

Для отправки сообщения по электронной почте программа отправит SMS на специальный номер оператора МТС (Россия). Оператор МТС (Россия) отправит новый номер телефона на ваш адрес электронной почты. Деньги за отправку SMS на специальный номер списываются с мобильного счета, соответствующего текущей установленной SIM-карте.

➤ *Чтобы при замене SIM-карты или включении вашего устройства без нее вы могли узнать новый номер телефона, а также заблокировать устройство, предварительно выполните следующие действия:*

1. В главном окне Kaspersky Mobile Security нажмите **Анти-Вор > Настройка**.
2. Установите флажок **SIM-Контроль**.
3. В блоке **Способы получения нового номера телефона и местоположения устройства** заполните поля **Номер телефона** и **Адрес электронной почты**, чтобы получать новый номер телефона при замене SIM-карты по SMS или по электронной почте.
4. Если требуется, в блоке **Параметры блокирования** установите флажок **Блокировать при смене SIM-карты**, чтобы заблокировать устройство при замене SIM-карты или включении без нее.
5. Если требуется, в поле **Текст при блокировании** введите текст сообщения, которое будет отображаться на экране заблокированного устройства.

## КАК ДИСТАНЦИОННО ЗАБЛОКИРОВАТЬ УСТРОЙСТВО И УЗНАТЬ ЕГО МЕСТОПОЛОЖЕНИЕ

При краже или потере вашего устройства вы можете заблокировать устройство и получить координаты его местоположения при помощи веб-портала <https://anti-theft.kaspersky.com> или SMS-команды `find: <код>` (где <код> – это секретный код Kaspersky Mobile Security на вашем устройстве).

*Отправка SMS-команды на ваше устройство оплачивается согласно тарифу оператора сотовой связи, используемого на другом мобильном устройстве.*

Дистанционное блокирование и определение местоположения устройства возможно, если выполнены следующие условия: программа Kaspersky Mobile Security установлена в качестве администратора устройства, сигнал сотовой связи есть на устройстве и дистанционный запуск этой функции разрешен на устройстве.

«Лаборатория Касперского» также рекомендует разрешить использование GPS в настройках устройства, чтобы программа могла определять местонахождение устройства с помощью GPS.

➤ *Чтобы заблокировать свое устройство и получить координаты его местоположения на карте через <https://anti-theft.kaspersky.com>, 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, которую вы использовали при первоначальной настройке программы.

Если вы забыли пароль, вы можете его восстановить.

3. Выберите закладку с названием того устройства, которое хотите заблокировать и найти.
4. Нажмите на кнопку **Блокирование и Поиск**.
5. Если требуется, в блоке **Блокирование и Поиск** введите текст, который будет отображаться на экране заблокированного устройства. Также введите адрес электронной почты, на который вы хотите получить местоположение устройства на карте.
6. Нажмите на кнопку **Заблокировать и найти**.

Запуск Блокирования и Поиска одной командой через веб-портал будет доступен позже официального выпуска новой версии Kaspersky Mobile Security. Через необновленный веб-портал вы можете запустить Блокирование и Поиск двумя командами.

Когда Kaspersky Mobile Security обнаружит ваше устройство, вы увидите его координаты на портале, а также получите их на адрес электронной почты.

На веб-портале вы можете посмотреть только последнее обнаруженное местоположение устройства на карте. Предыдущие GPS-координаты устройства остаются в полученном сообщении электронной почты и удаляются с веб-портала.

- ◆ Чтобы заблокировать свое устройство и получить координаты его местоположения при помощи SMS-команды, выполните одно из следующих действий:
  - Сформируйте и отправьте команду на свое устройство из Kaspersky Mobile Security с помощью функции отправки SMS-команды, если программа установлена на другом устройстве (см. раздел «Как отправить SMS-команды с другого устройства, на котором установлена Kaspersky Mobile Security» на стр. 28). При формировании SMS-команды используйте секретный код Kaspersky Mobile Security, установленной на вашем устройстве.
  - Отправьте SMS на ваше устройство со следующим специальным текстом `find: <код>` (где <код> – это секретный код Kaspersky Mobile Security на вашем устройстве).

## КАК ДИСТАНЦИОННО ВКЛЮЧИТЬ СИРЕНУ НА УСТРОЙСТВЕ

При краже или потере вашего устройства вы можете дистанционно включить сирену на устройстве (даже, если звук на устройстве выключен) и заблокировать устройство при помощи веб-портала <https://anti-theft.kaspersky.com> или SMS-команды `alarm: <код>` (где <код> – это секретный код Kaspersky Mobile Security на вашем устройстве).

Отправка SMS-команды на ваше устройство оплачивается согласно тарифу оператора сотовой связи, используемого на другом мобильном устройстве.

Дистанционное включение сирены возможно, если выполнены следующие условия: сигнал сотовой связи есть на устройстве и дистанционный запуск этой функции разрешен на устройстве.

- ◆ Чтобы включить сирену на устройстве и заблокировать его через <https://anti-theft.kaspersky.com>, 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, которую вы использовали при первоначальной настройке программы.

Если вы забыли пароль, вы можете его восстановить.

3. Выберите закладку с названием того устройства, на котором хотите включить сирену и которое хотите заблокировать.
4. Нажмите на кнопку **Сирена**.
5. Если требуется, в блоке **Сирена** введите текст, который будет отображаться на экране заблокированного устройства.
6. Нажмите на кнопку **Включить сирену**.

Включение Си́рены через веб-портал будет доступно позже официального выпуска новой версии Kaspersky Mobile Security.

- Чтобы включить сирену на устройстве и заблокировать его при помощи SMS-команды, выполните одно из следующих действий:
  - Сформируйте и отправьте команду на свое устройство из Kaspersky Mobile Security с помощью функции отправки SMS-команды, если программа установлена на другом устройстве (см. раздел «Как отправить SMS-команды с другого устройства, на котором установлена Kaspersky Mobile Security» на стр. 28). При формировании SMS-команды используйте секретный код Kaspersky Mobile Security, установленной на вашем устройстве.
  - Отправьте SMS на ваше устройство со следующим специальным текстом `alarm: <код>` (где <код> – это секретный код Kaspersky Mobile Security на вашем устройстве).

## КАК УДАЛИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ С УСТРОЙСТВА ИЛИ ПОЛНОСТЬЮ ОТФОРМАТИРОВАТЬ ЕГО

При краже или потере вашего устройства вы можете удалить данные с него, чтобы они не попали в чужие руки.

Вы можете удалить следующую информацию:

- персональные данные (например, контакты, переписку и данные об учетной записи Google™) и данные на карте памяти;
- все данные, включая данные на карте памяти.

Вы можете дистанционно удалить данные с устройства, используя <https://anti-theft.kaspersky.com> или отправив специальные SMS-команды.

Отправка SMS-команды на ваше устройство оплачивается согласно тарифу оператора сотовой связи, используемого на другом мобильном устройстве.

Дистанционное удаление данных возможно, если выполнены следующие условия: программа Kaspersky Mobile Security установлена в качестве администратора устройства, сигнал сотовой связи есть на устройстве и дистанционный запуск этой функции разрешен на устройстве.

- Чтобы дистанционно удалить данные с устройства через <https://anti-theft.kaspersky.com>, 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, которую вы использовали при первоначальной настройке программы.  
  
Если вы забыли пароль, вы можете его восстановить.
  3. Выберите закладку с названием того устройства, с которого хотите удалить данные.

4. Нажмите на кнопку **Удаление данных**.
5. В блоке **Удаление данных** выберите данные, которые вы хотите удалить с устройства.
  - Чтобы удалить персональные данные (например, учетную запись Google, контакты и переписку) и отформатировать карту памяти, выберите **Только личная информация**.
  - Чтобы удалить все данные, включая данные на карте памяти, и вернуть устройство к заводским настройкам, выберите **Все данные с вашего устройства**.

После того, как все данные будут удалены с устройства, программа Kaspersky Mobile Security также будет удалена. Устройство не сможет больше выполнять дистанционные команды.

6. Нажмите на кнопку **Удалить**.

Обновленный веб-портал будет доступен позже официального выпуска новой версии Kaspersky Mobile Security.

➤ Чтобы дистанционно удалить данные со своего устройства при помощи SMS-команд, выполните одно из следующих действий:

- Сформируйте и отправьте команду на свое устройство из Kaspersky Mobile Security с помощью функции отправки SMS-команды, если программа установлена на другом устройстве (см. раздел «Как отправить SMS-команды с другого устройства, на котором установлена Kaspersky Mobile Security» на стр. 28). Вы можете выбрать удаление персональных данных или всех данных. При формировании SMS-команды используйте секретный код Kaspersky Mobile Security, установленной на вашем устройстве.
- Отправьте SMS на ваше устройство со следующим специальным текстом:
  - wipe: <код> – для удаления персональных данных и данных на карте памяти;
  - fullreset: <код> – для удаления всех данных с устройства и возврата устройства к заводским настройкам.

<Код> – это секретный код Kaspersky Mobile Security на вашем устройстве.

## КАК ПОЛУЧИТЬ ФОТОГРАФИИ ЧЕЛОВЕКА, КОТОРЫЙ СЕЙЧАС ИСПОЛЬЗУЕТ ВАШЕ УСТРОЙСТВО

При краже или потере устройства вы можете дистанционно получить фотографии человека, который в настоящее время использует ваше устройство, а также заблокировать устройство.

Функция работает, если ваше устройство оборудовано фронтальной камерой.

Вы можете отправить команду сделать фотографии человека, который сейчас пользуется устройством, только через веб-портал <https://anti-theft.kaspersky.com>. Отправка такой команды по SMS не поддерживается.

Дистанционный запуск функции Анти-Вора возможен, если выполнены следующие условия: программа Kaspersky Mobile Security установлена в качестве администратора устройства, сигнал сотовой связи есть на устройстве и дистанционный запуск этой функции разрешен на устройстве.

➤ Чтобы получить фотографии человека, который сейчас использует ваше устройство, 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, которую вы использовали при первоначальной настройке программы.

Если вы забыли пароль, вы можете его восстановить.

3. Выберите закладку с названием того устройства, с которого хотите получить фотографии и которое хотите заблокировать.
4. Нажмите на кнопку **Тайное фото**.
5. Если потребуется, в блоке **Тайное фото** введите текст, который будет отображаться на экране заблокированного устройства.
6. Нажмите на кнопку **Получить фото**.

Обновленный веб-портал будет доступен позже официального выпуска новой версии Kaspersky Mobile Security.

## КАК ИЗБАВИТЬСЯ ОТ НЕЖЕЛАТЕЛЬНЫХ ВЫЗОВОВ И SMS

Чтобы избавиться от нежелательных вызовов и SMS, вы можете использовать Фильтр вызовов и SMS, входящий в состав Kaspersky Mobile Security.

Фильтр вызовов и SMS блокирует нежелательные сообщения и вызовы на основе списка разрешенных и запрещенных контактов и в зависимости от выбранного режима.

► *Чтобы избавиться от нежелательных вызовов и SMS, выполните следующие действия:*

1. Определитесь, от каких контактов вы хотите блокировать вызовы и SMS, а от каких контактов разрешать. Для этого выберите режим фильтрации. В главном окне Kaspersky Mobile Security нажмите **Фильтр вызовов и SMS > Режим: <текущий режим фильтрации>**.
2. Выберите значение для параметра **Режим Фильтра вызовов и SMS**:
  - Чтобы блокировать вызовы и SMS только от запрещенных контактов и доставлять вызовы и SMS от остальных номеров, выберите **Запрещенные контакты**.
  - Чтобы блокировать вызовы и SMS от всех контактов и доставлять вызовы и SMS только от разрешенных контактов, выберите **Разрешенные контакты**.
  - Чтобы блокировать вызовы и SMS от запрещенных контактов и пропускать от разрешенных контактов, выберите **Стандартный**.
3. Если потребуется, включите дополнительные параметры фильтрации.

Например, если вы выбрали режим фильтрации **Разрешенные контакты** или **Стандартный**, вы можете автоматически разрешить вызовы и SMS от контактов из телефонной книги устройства, независимо выбранного режима фильтрации. Для этого установите флажок **Разрешать Контакты**.

Если вы выбрали режим фильтрации **Запрещенные контакты** или **Стандартный**, вы можете автоматически запретить SMS с номеров, содержащих буквы, независимо от выбранного режима фильтрации. Для этого установите флажок **Блокировать нечисловые номера**.

4. В зависимости от выбранного режима сформируйте список разрешенных и запрещенных контактов:
- Чтобы сформировать список запрещенных контактов, вернитесь в главное окно Kaspersky Mobile Security. В главном окне нажмите **Фильтр вызовов и SMS > Запрещенные контакты**.
  - Чтобы сформировать список разрешенных контактов, вернитесь в главное окно Kaspersky Mobile Security. В главном окне нажмите **Фильтр вызовов и SMS > Разрешенные контакты**.

## КАК ЗАЩИТИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ОТ КРАЖИ В СЕТИ

Чтобы защитить ваши персональные данные от кражи в сети, вы можете использовать Веб-Фильтр и SMS Анти-Фишинг, входящие в состав Kaspersky Mobile Security.

**Веб-Фильтр и SMS Анти-Фишинг доступны только в коммерческой версии Kaspersky Mobile Security.**

Веб-Фильтр блокирует вредоносные веб-сайты, цель которых – распространить вредоносный код, а также поддельные (фишинговые) веб-сайты, цель которых – украсть ваши конфиденциальные данные, такие как пароли от онлайн-банков, онлайн-аукционов или систем оплаты, и получить доступ к вашим финансовым счетам.

SMS Анти-Фишинг блокирует ссылки в SMS на вредоносные и поддельные веб-сайты.

**Веб-Фильтр проверяет веб-сайты только в стандартном браузере Android и не проверяет их в других браузерах.**

Вы можете запустить стандартный браузер Android из Kaspersky Mobile Security или из меню приложений вашего устройства. Если Веб-Фильтр включен, он будет блокировать поддельные веб-сайты до их открытия.

➤ *Чтобы включить постоянную проверку веб-сайтов, выполните следующие действия:*

1. В главном окне Kaspersky Mobile Security нажмите **Веб-Фильтр**.
2. Установите переключатель **Веб-Фильтр** в состояние **включен**.

При включении Веб-Фильтр автоматически проверяет, какой браузер установлен по умолчанию. Если Веб-Фильтр не поддерживает текущий браузер, установленный по умолчанию, Веб-Фильтр предложит вам изменить его на стандартный браузер Android.

Для постоянной проверки веб-сайтов рекомендуется установить стандартный браузер Android в качестве браузера по умолчанию.

**Если вы не хотите изменять текущий браузер по умолчанию, для безопасной работы с персональными данными в сети запускайте стандартный браузер Android.**

➤ *Чтобы безопасно работать с персональными данными в сети и блокировать вредоносные веб-сайты, выполните следующее:*

В главном окне Kaspersky Mobile Security нажмите **Веб-Фильтр > Открыть браузер**.

➤ *Чтобы включить проверку ссылок в SMS, выполните следующие действия:*

1. В главном окне Kaspersky Mobile Security нажмите **Веб-Фильтр**.
2. Установите переключатель **SMS Анти-Фишинг** в состояние **включен**.

## КАК ПОСМОТРЕТЬ ОТЧЕТЫ О РАБОТЕ ПРОГРАММЫ

События, которые происходят в ходе работы Антивируса, Веб-Фильтра, Фильтра вызовов и SMS, фиксируются в отчетах.

Отчеты сгруппированы по времени создания. Вы можете выбрать отображение отчетов по одному компоненту программы. Отчеты сохраняются до достижения 50 записей. После того как число записей в отчете превысит 50, более ранние записи удаляются и замещаются новыми.

➤ *Чтобы посмотреть отчеты о работе программы, выполните следующее:*

В главном окне Kaspersky Mobile Security нажмите **Дополнительно > Отчеты**.

## КАК ИЗМЕНИТЬ СЕКРЕТНЫЙ КОД ПРОГРАММЫ

Секретный код используется в следующих целях:

- чтобы предотвратить несанкционированный доступ к параметрам программы;
- чтобы дистанционно с другого устройства запустить функции Анти-Вора и скрытие контактов.

Вы устанавливаете секретный код при первой настройке программы, но в дальнейшем вы можете его изменить.

➤ *Чтобы изменить секретный код программы, выполните следующие действия:*

1. В главном окне Kaspersky Mobile Security нажмите **Дополнительно > Изменение секретного кода**.
2. Введите текущий секретный код программы в поле **Введите текущий секретный код** и нажмите **Далее**.
3. Введите новый секретный код программы в поле **Придумайте новый секретный код** и нажмите **Далее**.
4. Введите этот код еще раз в поле **Повторно введите новый код** и нажмите **Вход**.

## КАК ВОССТАНОВИТЬ СЕКРЕТНЫЙ КОД ПРОГРАММЫ

➤ *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, 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 специальный код, который позволяет безопасно восстановить секретный код программы.
5. Запустите Kaspersky Mobile Security на устройстве.
6. Нажмите **Меню > Восстановление секретного кода**.
7. Введите код восстановления, указанный на веб-портале.  
На экране устройства отобразится ваш секретный код.
8. Введите ваш восстановленный секретный код.

# ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Этот раздел содержит информацию о способах получения технической поддержки и о том, какие условия требуются для получения помощи от Службы технической поддержки.

## В ЭТОМ РАЗДЕЛЕ

---

Способы получения технической поддержки .....	<a href="#">37</a>
Техническая поддержка по телефону .....	<a href="#">37</a>
Получение технической поддержки через Личный кабинет .....	<a href="#">37</a>

## СПОСОБЫ ПОЛУЧЕНИЯ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Если вы не нашли решения вашей проблемы в документации к программе или в одном из источников информации о программе (см. раздел «Источники информации о программе» на стр. [8](#)), рекомендуем обратиться в Службу технической поддержки «Лаборатории Касперского». Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (<http://support.kaspersky.ru/support/rules>).

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

- Позвонить по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или интернациональной Службы технической поддержки.
- Отправить запрос из Личного кабинета на веб-сайте Службы технической поддержки. Этот способ позволяет вам связаться со специалистами Службы технической поддержки через форму запроса.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Техническая поддержка для владельцев пробных лицензий не осуществляется.

## ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ПО ТЕЛЕФОНУ

Если возникла неотложная проблема, вы можете позвонить специалистам русскоязычной или международной технической поддержки (<http://support.kaspersky.ru/support/international>).

Перед обращением в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами предоставления поддержки (<http://support.kaspersky.ru/support/details>). Это позволит нашим специалистам быстрее помочь вам.

## ПОЛУЧЕНИЕ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ ЧЕРЕЗ ЛИЧНЫЙ КАБИНЕТ

*Личный кабинет* – это ваш персональный раздел (<https://my.kaspersky.ru>) на сайте Службы технической поддержки.

Для доступа к Личному кабинету вам требуется зарегистрироваться на странице регистрации (<https://my.kaspersky.com/ru/registration>). Вам нужно указать адрес электронной почты и пароль для доступа в Личный кабинет.

В Личном кабинете вы можете выполнять следующие действия:

- отправлять запросы в Службу технической поддержки и Антивирусную лабораторию;
- обмениваться сообщениями со Службой технической поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени;
- просматривать полную историю ваших запросов в Службу технической поддержки;
- получать копию файла ключа в случае, если файл ключа был утерян или удален.

### Электронный запрос в Службу технической поддержки

Вы можете отправить электронный запрос в Службу технической поддержки на русском, английском, немецком, французском или испанском языках.

В полях формы электронного запроса вам нужно указать следующие сведения:

- тип запроса;
- название и номер версии программы;
- текст запроса;
- номер клиента и пароль;
- электронный адрес.

Специалист Службы технической поддержки направляет ответ на ваш вопрос в ваш Личный кабинет и по адресу электронной почты, который вы указали в электронном запросе.

### Электронный запрос в Антивирусную лабораторию

Некоторые запросы требуется направлять не в Службу технической поддержки, а в Антивирусную лабораторию.

Вы можете направлять в Антивирусную лабораторию запросы следующих типов:

- *Неизвестная вредоносная программа* – вы подозреваете, что файл содержит вирус, но Kaspersky Mobile Security не обнаруживает его в качестве зараженного.

Специалисты Антивирусной лаборатории анализируют присылаемый вредоносный код и при обнаружении неизвестного ранее вируса добавляют его описание в базу данных, доступную при обновлении антивирусных программ.

- *Ложное срабатывание антивируса* – Kaspersky Mobile Security определяет файл как содержащий вирус, но вы уверены, что файл не является вирусом.
- *Запрос на описание вредоносной программы* – вы хотите получить описание вируса, обнаруженного Kaspersky Mobile Security, на основе названия этого вируса.

Вы также можете направлять запросы в Антивирусную лабораторию со страницы с формой запроса (<http://support.kaspersky.ru/virlab/helpdesk.html>), не регистрируясь в Личном кабинете. При этом вам не требуется указывать код активации программы.

# ГЛОССАРИЙ

## К

### **KASPERSKY SECURITY NETWORK (KSN)**

Инфраструктура онлайн-служб и сервисов, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ «Лаборатории Касперского» на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

## А

### **АКТИВАЦИЯ ПРОГРАММЫ**

Перевод программы в полнофункциональный режим. Активация выполняется пользователем во время или после установки программы. Для активации программы пользователю необходимо код активации.

### **АНТИВИРУСНЫЕ БАЗЫ**

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных «Лаборатории Касперского» на момент выпуска баз. Записи в базах позволяют обнаруживать в проверяемых объектах вредоносный код. Базы формируются специалистами «Лаборатории Касперского» и обновляются каждый час.

### **АРХИВ**

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

## З

### **ЗАПРЕЩЕННЫЙ СПИСОК**

Записи списка содержат следующую информацию:

- *Номер телефона*, с которого Фильтр вызовов и SMS блокирует вызовы и (или) SMS.
- *Тип событий*, которые Фильтр вызовов и SMS блокирует с этого номера. Представлены следующие типы событий: вызовы и SMS, только вызовы, только SMS.
- *Ключевая фраза*, по которой Фильтр вызовов и SMS определяет, что SMS является нежелательным (спамом). Фильтр вызовов и SMS блокирует только те SMS, которые содержат эту ключевую фразу, остальные SMS Фильтр вызовов и SMS доставляет.

### **ЗАРАЖЕННЫЙ ОБЪЕКТ**

Объект, участок кода которого полностью совпадает с участком кода известной программы, предоставляющей угрозу. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами.

## К

### **КОД АКТИВАЦИИ**

Код, который вы получаете, приобретая коммерческую лицензию Kaspersky Mobile Security. Этот код необходим для активации программы.

Код активации представляет собой последовательность из двадцати латинских букв и цифр, в формате xxxxx-xxxxx-xxxxx.

**Л****ЛЕЧЕНИЕ ОБЪЕКТОВ**

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

**Н****НЕЧИСЛОВОЙ НОМЕР**

Номер телефона, который включает в себя буквы или полностью состоит из них.

**О****ОБНОВЛЕНИЕ БАЗ**

Одна из функций, выполняемых программой «Лаборатории Касперского», которая позволяет поддерживать защиту в актуальном состоянии. При этом происходит копирование антивирусных баз с серверов обновлений «Лаборатории Касперского» на устройство и автоматическое подключение их к программе.

**Р****РАЗРЕШЕННЫЙ СПИСОК**

Записи этого списка содержат следующую информацию:

- *Номер телефона*, с которого Фильтр вызовов и SMS доставляет вызовы и (или) SMS.
- *Тип событий*, которые Фильтр вызовов и SMS доставляет с этого номера. Представлены следующие типы событий: вызовы и SMS, только вызовы, только SMS.
- *Ключевая фраза*, по которой Фильтр вызовов и SMS определяет, что SMS является желательным (не спамом). Фильтр вызовов и SMS доставляет только те SMS, которые содержат эту ключевую фразу, остальные SMS Фильтр вызовов и SMS блокирует.

**С****СЕКРЕТНЫЙ КОД ПРОГРАММЫ**

Секретный код программы используется, чтобы предотвратить несанкционированный доступ к параметрам программы и к защищаемой на устройстве информации. Он задается пользователем при первом запуске программы и состоит не менее чем из четырех цифр. Секретный код программы необходим в следующих случаях:

- для доступа к параметрам программы;
- при отправке с другого устройства SMS-команды на свое устройство, чтобы дистанционно запустить функции Анти-Вора или скрыть конфиденциальные контакты и связанную с ними информацию.

**СРОК ДЕЙСТВИЯ ЛИЦЕНЗИИ**

Срок действия лицензии – период времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

**У****УДАЛЕНИЕ ОБЪЕКТА**

Способ обработки объекта, при котором происходит его безвозвратное удаление с того места, где он был обнаружен программой. Такой способ обработки рекомендуется применять к опасным объектам, лечение которых по тем или иным причинам невозможно.

# ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» – известный в мире производитель систем защиты компьютеров от угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году «Лаборатория Касперского» вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности для конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). По результатам исследования КОМКОН TGI-Russia 2009, «Лаборатория Касперского» – самый предпочитаемый производитель систем защиты для домашних пользователей в России.

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с центральным офисом в Москве и пятью региональными дивизионами, управляющими деятельностью компании в России, Западной и Восточной Европе, на Ближнем Востоке, в Африке, в Северной и Южной Америке, в Японии, Китае и других странах Азиатско-Тихоокеанского региона. В компании работает более 2000 квалифицированных специалистов.

**Продукты.** Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает антивирусные приложения для настольных компьютеров и ноутбуков, для карманных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает программы и сервисы для защиты рабочих станций, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации от компьютерных угроз. Продукты «Лаборатории Касперского» сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни новых компьютерных угроз, создают средства их обнаружения и лечения и включают их в базы, используемые программами «Лаборатории Касперского». *Антивирусная база «Лаборатории Касперского» обновляется ежедневно, база Анти-Спама – каждые 5 минут.*

**Технологии.** Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно «Лабораторией Касперского». Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: среди них SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Многие из инновационных технологий компании подтверждены патентами.

**Достижения.** За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2010 году Антивирус Касперского получил несколько высших наград Advanced+ в тестах, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 300 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 200 тысяч.

Веб-сайт «Лаборатории Касперского»:

<http://www.kaspersky.ru>

Вирусная энциклопедия:

<http://www.securelist.com/ru/>

Антивирусная лаборатория:

[newvirus@kaspersky.com](mailto:newvirus@kaspersky.com) (только для отправки возможно зараженных файлов в архивированном виде)

<http://support.kaspersky.ru/virlab/helpdesk.html>

(для запросов вирусным аналитикам)

Веб-форум «Лаборатории Касперского»:

<http://forum.kaspersky.com>

# ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

Информация о стороннем коде содержится в блоке **О программе**, расположенном в параметрах программы.

# УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Android и Google – товарные знаки Google, Inc.

# ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

## К

Kaspersky Account .....26

## А

Активация программы .....21  
код активации..... 18, 21  
купить код активации онлайн.....21  
лицензия.....17  
Анти-Вор.....26, 28, 30, 31, 32, 33  
SIM-Контроль .....30  
Блокирование и Поиск.....26, 30  
Сирена .....31  
Тайное фото.....33  
Удаление данных.....26, 32

## Б

Блокирование  
входящие SMS .....34  
входящие вызовы .....34

## В

Веб-Фильтр .....35  
Виджет главного экрана.....15

## Г

Главное окно программы .....13

## З

ЗАО «Лаборатория Касперского» .....42  
Запуск  
обновление вручную.....23, 24  
проверка устройства вручную.....22, 23  
проверка устройства по расписанию.....23  
программа .....19  
Зараженный объект.....40  
Значок в строке состояния.....13

## К

Код  
восстановить секретный код.....36  
изменить секретный код программы .....36  
код активации.....18

## Л

Лицензионное соглашение .....17  
Лицензия  
активация программы.....21  
информация .....22  
код активации.....18  
Лицензионное соглашение.....17, 21, 22  
продление .....21  
продлить онлайн.....21  
Личные контакты .....24, 25

дистанционный запуск.....	25
<b>О</b>	
Обновление	
запуск вручную.....	23
запуск по расписанию.....	24
Определение местоположения устройства.....	26, 30
Отправка SMS-команды.....	25, 26, 28
Отчеты.....	36
<b>П</b>	
Проверка по требованию.....	22, 23
Продление срока действия лицензии.....	21
<b>Р</b>	
Расписание	
Обновление.....	24
Проверка по требованию.....	23
<b>С</b>	
Секретный код программы.....	36
Сирена.....	31
<b>У</b>	
Уведомления программы.....	16
<b>Ф</b>	
Фильтр вызовов и SMS.....	34