

Kaspersky Internet Security для Android

**KASPERSKY** для Android

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: 6/26/2013

© ЗАО «Лаборатория Касперского», 2013

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

# СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ .....	5
В этом документе.....	5
Условные обозначения.....	7
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 .....	10
KASPERSKY INTERNET SECURITY.....	11
Что нового .....	12
Аппаратные и программные требования .....	12
Комплект поставки.....	13
Сервис для пользователей .....	13
УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ .....	14
Установка программы.....	14
Удаление программы .....	14
ИНТЕРФЕЙС ПРОГРАММЫ .....	15
Главное окно Kaspersky Internet Security .....	15
Индикатор состояния защиты в виде щита.....	16
Панель быстрого запуска .....	17
Значок в области уведомлений .....	18
Виджет для главного экрана устройства.....	19
Уведомления.....	19
ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ.....	21
О Лицензионном соглашении .....	21
О лицензии .....	21
О коде активации.....	22
ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ.....	23
БЫСТРЫЙ СТАРТ .....	24
Что делать, если обнаружен вредоносный объект .....	24
Как защитить данные от несанкционированного доступа .....	24
Зачем нужен секретный код .....	25
Что такое Kaspersky Account .....	25
Первоначальная настройка Анти-Вора .....	26
Что делать, если устройство потеряно или украдено.....	26
РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ .....	28
Сканер (Антивирус).....	28
Полная проверка устройства .....	29
Быстрая проверка .....	29
Проверка папок и файлов.....	29
Автоматическая проверка по расписанию .....	30
Обновление антивирусных баз и версий программы.....	30

Автоматическое обновление по расписанию.....	30
Личные контакты.....	31
Скрытие информации для контактов.....	32
Дистанционный запуск скрытия с другого устройства.....	32
Анти-Вор.....	32
Добавление устройства в учетную запись на веб-портале.....	33
Отправка SMS-команд из Kaspersky Internet Security.....	33
Дистанционный контроль SIM-карты.....	34
Дистанционное блокирование и поиск устройства.....	34
Дистанционное включение сирены на устройстве.....	35
Дистанционное удаление данных с устройства.....	36
Дистанционное фотографирование.....	37
Фильтр вызовов и SMS.....	38
Стандартная фильтрация контактов.....	38
Блокирование всех контактов, кроме разрешенных.....	39
Блокирование только запрещенных контактов.....	39
Веб-Фильтр и SMS Анти-Фишинг.....	40
Постоянная проверка веб-сайтов.....	40
Постоянная проверка ссылок в SMS.....	40
Другие задачи.....	41
Приобретение лицензии и продление срока ее действия.....	41
Активация полной версии программы.....	42
Просмотр информации о лицензии, сроке ее действия.....	42
Просмотр отчетов о работе программы.....	42
Изменение секретного кода программы.....	43
Восстановление секретного кода программы.....	43
ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ.....	44
Способы получения технической поддержки.....	44
Техническая поддержка по телефону.....	44
Получение технической поддержки через Личный кабинет.....	44
ГЛОССАРИЙ.....	46
ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО».....	48
ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ.....	49
УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ.....	50
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ.....	51

# ОБ ЭТОМ РУКОВОДСТВЕ

Этот документ представляет собой Руководство пользователя Kaspersky Internet Security для Android (далее Kaspersky Internet Security).

Руководство пользователя адресовано пользователям Kaspersky Internet 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 Internet Security.
- Рассказать о дополнительных источниках информации о программе и способах получения технической поддержки.

## В ЭТОМ РАЗДЕЛЕ

---

В этом документе .....	<a href="#">5</a>
Условные обозначения .....	<a href="#">7</a>

## 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 Internet 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.

### Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Internet Security.

### Интерфейс программы

Этот раздел содержит информацию об основных элементах графического интерфейса программы: главном окне, индикаторе состояния защиты в виде щита, панели быстрого запуска, значке программы, 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, 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.

## Быстрый старт

Этот раздел содержит информацию для быстрого начала работы с программой после ее установки:

- сведения об основных возможностях программы;
- инструкции о действиях в случае обнаружения вредоносного объекта;
- сведения о том, как защитить свои данные от несанкционированного доступа;
- инструкции о действиях в случае потери или кражи устройства.

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

# 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="#">10</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. [44](#)).

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/android-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://support.kaspersky.ru/mobile/kisandroid> 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 Internet 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 справки.

Контекстная справка содержит сведения о каждом окне программы: перечень и описание параметров и список решаемых задач.

Полная справка содержит подробную информацию о том, как управлять защитой, настраивать параметры программы и решать основные задачи пользователя.

## 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 Internet Security для Android».

# KASPERSKY INTERNET SECURITY

Kaspersky Internet Security обладает следующими основными возможностями:

## Защита от вирусов и других вредоносных программ

Для защиты вашего устройства от вирусов и других вредоносных программ используется компонент Сканер (Антивирус).

В бесплатной версии программы компонент называется Сканер, в полной версии – Антивирус.

С помощью Сканера вы можете только 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.

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.

## Скрытие личных контактов, истории разговоров и SMS-переписки с ними

Для скрытия личных контактов и связанной с ними информации используется компонент Личные контакты.

Компонент Личные контакты доступен только в полной версии Kaspersky Internet Security и на устройствах с установленной SIM-картой.

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

## Защита данных при потере или краже устройства

Для защиты информации от попадания в чужие руки, а также для поиска устройства при его потере или краже используется компонент Анти-Вор.

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>. Также, если устройство поддерживает SIM-карту, то 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.

## Блокирование нежелательных вызовов и SMS

Для блокирования нежелательных входящих вызовов и SMS используется компонент Фильтр вызовов и SMS.

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

## Защита от интернет-угроз

Для защиты от интернет-угроз используются компоненты Веб-Фильтр и SMS Анти-Фишинг.

Компоненты Веб-Фильтр и SMS Анти-Фишинг доступны только в полной версии Kaspersky Internet Security.

Компонент SMS Анти-Фишинг доступен только на устройствах с установленной SIM-картой.

Веб-Фильтр блокирует вредоносные веб-сайты, цель которых – распространить вредоносный код, а также поддельные (фишинговые) веб-сайты, цель которых – украсть ваши конфиденциальные данные и получить доступ к вашим финансовым счетам.

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

### В ЭТОМ РАЗДЕЛЕ

Что нового .....	<a href="#">12</a>
Аппаратные и программные требования.....	<a href="#">12</a>
Комплект поставки.....	<a href="#">13</a>
Сервис для пользователей.....	<a href="#">13</a>

## ЧТО НОВОГО

В Kaspersky Internet Security появились следующие новые возможности:

- Одна программа для планшетов и смартфонов.
- Переработан пользовательский интерфейс.
- Добавлено окно статуса защиты устройства, которое предоставляет следующие возможности:
  - Просмотр в одном окне всех проблем, связанных с безопасностью устройства, а также их устранение в одно действие.
  - Просмотр информации о выполненных проверках, обновлении антивирусных баз, используемой версии программы.
- Включение Сирены через веб-портал.
- Запуск Блокирования и Поиска одной командой через веб-портал.

## АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ

Для функционирования Kaspersky Internet Security устройство должно удовлетворять следующим требованиям:

- Смартфон или планшет с разрешением экрана от 320x480 пикселей.
- 15 МБ свободного места в основной памяти устройства.
- Операционная система Android™ 2.3.x – 4.2.x.

Программа устанавливается только в основную память устройства.

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

## 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.
- **Через Google Play.** Загружается на устройство из сервиса Google Play.

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

- запечатанный конверт с QR-кодом для загрузки программы;
- 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 Internet Security через интернет-магазин, вы копируете программу с сайта интернет-магазина. Информация, необходимая для активации программы, в том числе код активации, 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 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.

# УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Internet Security.

## В ЭТОМ РАЗДЕЛЕ

---

Установка программы ..... [14](#)

Удаление программы ..... [14](#)

## УСТАНОВКА ПРОГРАММЫ

Установку Kaspersky Internet Security можно осуществить из Google Play, а также из дистрибутива программы на устройстве.

➤ *Чтобы установить Kaspersky Internet Security из Google Play, выполните следующие действия:*

1. Откройте Google Play и найдите в списке программ Kaspersky Internet Security.
2. Нажмите **Установить** или **Купить** в зависимости от версии программы.

Программа будет установлена автоматически с параметрами, рекомендованными специалистами «Лаборатории Касперского».

➤ *Чтобы установить Kaspersky Internet Security из дистрибутива, выполните следующие действия:*

1. Скопируйте дистрибутив программы на устройство. Для этого выполните одно из следующих действий:
  - Если дистрибутив программы ранее был загружен и сохранен на стационарном компьютере, подключите устройство к компьютеру и скопируйте на устройство дистрибутив программы.
  - На устройстве загрузите дистрибутив программы из интернет-магазина «Лаборатории Касперского» (<http://www.kaspersky.ru/store>).
2. Запустите установку программы. Для этого откройте APK-архив дистрибутива на устройстве.

Запустится мастер установки программы. По окончании работы мастера программа будет установлена с параметрами, рекомендованными специалистами «Лаборатории Касперского».

## УДАЛЕНИЕ ПРОГРАММЫ

➤ *Чтобы удалить Kaspersky Internet Security,*

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройки > Дополнительные настройки > Удаление программы**.
2. Введите секретный код программы.
3. Если вы забыли секретный код, вы можете его восстановить (см. раздел «Восстановление секретного кода программы» на стр. [43](#)).

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

# ИНТЕРФЕЙС ПРОГРАММЫ

Этот раздел содержит информацию об основных элементах графического интерфейса программы: главном окне, индикаторе состояния защиты в виде щита, панели быстрого запуска, значке программы, виджете и окнах уведомлений.

## В ЭТОМ РАЗДЕЛЕ

Главное окно Kaspersky Internet Security .....	<a href="#">15</a>
Индикатор состояния защиты в виде щита .....	<a href="#">16</a>
Панель быстрого запуска.....	<a href="#">17</a>
Значок в области уведомлений.....	<a href="#">18</a>
Виджет для главного экрана устройства .....	<a href="#">19</a>
Уведомления .....	<a href="#">19</a>

## ГЛАВНОЕ ОКНО KASPERSKY INTERNET SECURITY

Главное окно программы (см. рис ниже) содержит элементы интерфейса, предоставляющие доступ к основным функциям программы.

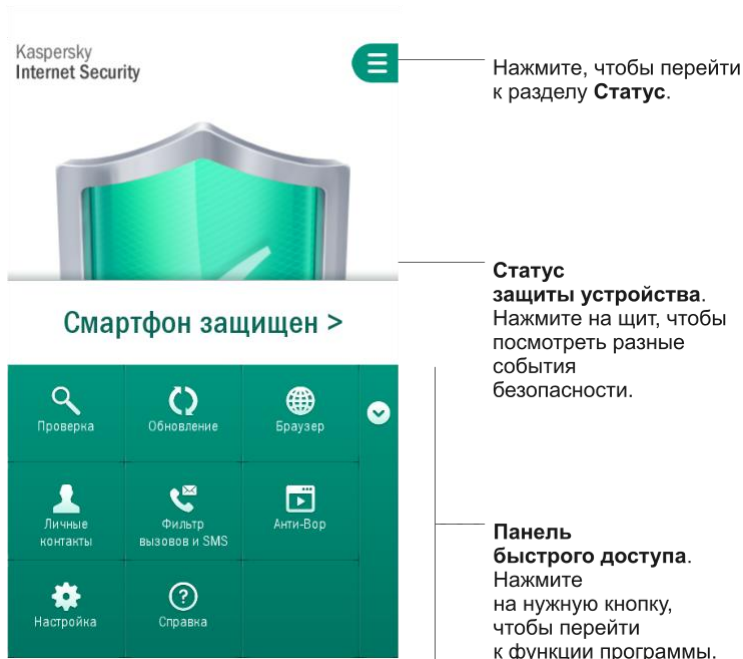


Рисунок 1. Главное окно

Количество кнопок на панели быстрого запуска может меняться в зависимости от доступных функций.

## Индикатор состояния защиты в виде щита

Индикатор состояния защиты выполнен в виде щита и расположен в центре главного окна программы (см. рис. ниже).



Рисунок 2. Щит в центре главного окна

Щит меняет цвет в зависимости от состояния защиты устройства:

- Зеленый – защита устройства обеспечена на должном уровне. Все компоненты защиты работают в соответствии с параметрами, рекомендуемыми специалистами «Лаборатории Касперского». Базы Kaspersky Internet Security своевременно обновлены. В результате проверки устройства не обнаружено вредоносных объектов или все обнаруженные вредоносные объекты обезврежены программой.
- Желтый – уровень защиты снижен, в работе Kaspersky Internet Security имеются некоторые проблемы. Например, проверка устройства не выполнялась более 14 дней или установлена новая непроверенная программа.
- Красный – есть проблемы, которые могут привести к заражению устройства и потере информации. Например, некоторые компоненты защиты приостановлены, антивирусные базы не обновлялись более 14 дней.



Нажав на щит в главном окне программы, вы можете открыть раздел **Статус** (см. рис. ниже). В разделе **Статус** приведена подробная информация о состоянии защиты устройства и предложены варианты действий для устранения проблем и угроз.

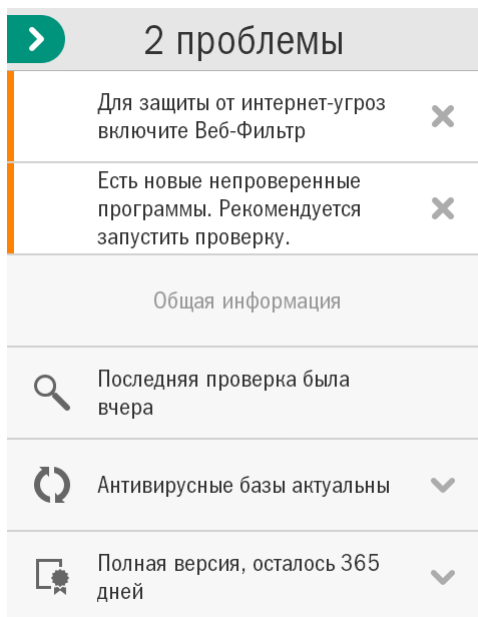


Рисунок 3. Раздел **Статус**

Проблемы в защите сгруппированы по категориям, к которым они относятся. Для каждой проблемы приведены действия, которые вы можете предпринять, чтобы решить проблему.

Проблемы в защите бывают двух типов:

- **Уведомительные.** Выделены желтым цветом. Уведомительные проблемы информируют о событиях, потенциально важных для обеспечения безопасности устройства (например, о том, что последняя проверка была выполнена более 14 дней назад или была установлена новая непроверенная программа). Уведомительную проблему можно скрыть, смахнув ее влево. После этого информация о проблеме будет доступна в меню **Скрытые проблемы**.
- **Критические.** Выделены красным цветом. Критические проблемы информируют о событиях, имеющих первостепенную важность для обеспечения безопасности устройства (например, вышла новая версия программы, антивирусные базы давно не обновлялись). Критическую проблему скрыть нельзя.

## ПАНЕЛЬ БЫСТРОГО ЗАПУСКА

Панель быстрого запуска позволяет перейти к основным функциям программы (см. рис. ниже).

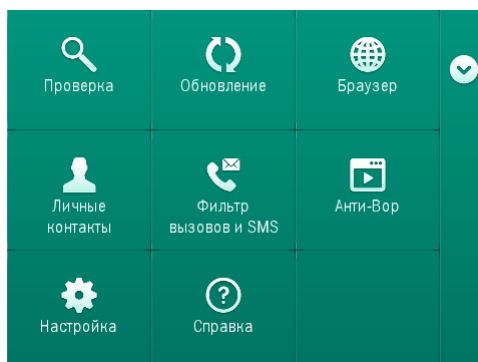











Рисунок 4. Панель быстрого запуска

По умолчанию панель быстрого запуска свернута. Вы можете развернуть панель быстрого запуска, потянув ее вверх или нажав на кнопку .

Количество кнопок на панели быстрого запуска может меняться в зависимости от доступных функций.

Значение каждой кнопки на панели быстрого запуска представлено в таблице ниже.

Таблица 2. Функции кнопок на панели быстрого запуска

Кнопка	Что означает
 (Проверка)	Позволяет запустить проверку всего устройства, только установленных программ, выбранной папки или файла.
 (Обновление)	Запускает обновление антивирусных баз программы, чтобы поддерживать защиту устройства в актуальном состоянии.
 (Браузер)	Открывает браузер Android по умолчанию с включенной проверкой веб-сайтов на наличие вирусов и фишинга.
 (Личные контакты)	Временно скрывает или отображает заранее выбранные личные контакты и информацию для них.
 (Фильтр вызовов и SMS)	Переходит к выбору режима фильтрации нежелательных вызовов и SMS.
 (Портал Анти-Вора)	Открывает веб-портал, чтобы дистанционно управлять функциями Анти-Вора на устройстве.
 (Настройка)	Открывает окно настройки параметров программы.
 (Справка)	Открывает справку программы.



## ЗНАЧОК В ОБЛАСТИ УВЕДОМЛЕНИЙ


После прохождения мастера первого запуска значок Kaspersky Internet Security появляется в строке состояния.

Значок служит индикатором работы программы и обеспечивает доступ к главному окну программы.

### Индикация работы программы

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

-  (цветной значок) – защита работает;
-  (черно-белый значок) – защита отключена;

-  (цветной значок с восклицательным знаком) – есть проблемы в защите. Например, антивирусные базы устарели или установлена новая непроверенная программа.

В бесплатной версии программы значок не отражает состояние защиты устройства.

### Доступ к главному окну программы

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

## ВИДЖЕТ ДЛЯ ГЛАВНОГО ЭКРАНА УСТРОЙСТВА

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



Рисунок 5. Виджет главного экрана

Виджет используется для перехода к главному окну программы.

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

Используется следующая цветовая индикация виджета:

- зеленый цвет щита означает, что защита включена;
- серый цвет щита означает, что защита выключена;
- 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 Internet 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 Internet Security выводит на экран в 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 объектом (см. рис. ниже). Программа предложит вам выбрать действие. Окно уведомления исчезнет с экрана только после того, как вы выберете одно из предложенных действий.

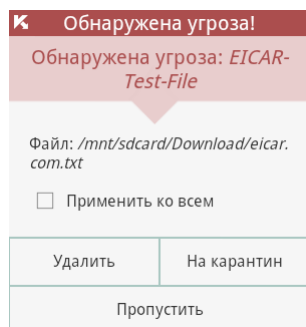


Рисунок 6. Окно уведомления

Всплывающие уведомления Kaspersky Internet 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 7. 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). Критические уведомления выделены красным цветом.
- **Важные** – информируют о событиях, потенциально важных для обеспечения безопасности устройства (например, о запуске проверки или обновления). Важные уведомления выделены зеленым цветом.
- **Информационные** – информируют о событиях, не имеющих первостепенной важности для обеспечения безопасности устройства. Информационные уведомления не выделяются цветом.

# ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

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

## В ЭТОМ РАЗДЕЛЕ

О Лицензионном соглашении .....	<a href="#">21</a>
О лицензии.....	<a href="#">21</a>
О коде активации.....	<a href="#">22</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. [13](#))

Объем предоставляемых услуг и срок использования программы зависят от версии программы.

Предусмотрены следующие версии программы:

- *Бесплатная версия.* Бесплатная версия позволяет использовать ограниченную функциональность Kaspersky Internet 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 полную версию программы.

- *Пробная версия.* Пробная версия позволяет использовать все функции программы в течение ознакомительного периода без выплаты вознаграждения.

С пробной версии вы можете перейти на полную версию или бесплатную версию программы. По истечении ознакомительного периода программа автоматически переключится на бесплатную версию.

- *Полная версия.* Полная версия предоставляет доступ ко всем функциям программы. Полная версия доступна после приобретения лицензии на использование программы. Лицензия имеет ограниченный срок действия.

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

По истечении срока действия лицензии программа автоматически переключится на бесплатную версию.

## О КОДЕ АКТИВАЦИИ

*Код активации* – это код, который вы получаете, приобретая лицензию на использование Kaspersky Internet Security. 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 Internet Security, код активации указан в документации или на коробке, в которой находится установочный компакт-диск.
- Если вы приобрели Kaspersky Internet 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 Internet 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 Internet Security запускается при старте операционной системы и защищает ваше устройство в течение всего сеанса работы.

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

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

# БЫСТРЫЙ СТАРТ

Этот раздел содержит информацию для быстрого начала работы с программой после ее установки:

- сведения об основных возможностях программы;
- инструкции о действиях в случае обнаружения вредоносного объекта;
- сведения о том, как защитить свои данные от несанкционированного доступа;
- инструкции о действиях в случае потери или кражи устройства.

## В ЭТОМ РАЗДЕЛЕ

---

Что делать, если обнаружен вредоносный объект .....	<a href="#">24</a>
Как защитить данные от несанкционированного доступа .....	<a href="#">24</a>
Что делать, если устройство потеряно или украдено .....	<a href="#">26</a>

## ЧТО ДЕЛАТЬ, ЕСЛИ ОБНАРУЖЕН ВРЕДОНОСНЫЙ ОБЪЕКТ

Если во время запуска приложения (например, игры) обнаружена угроза безопасности вашего устройства, то Kaspersky Internet Security предлагает вам выбрать действие над этим приложением. Вы можете выбрать одно из следующих действий:

- **На карантин** – программа помещает приложение на карантин.
- **Удалить** – программа удаляет приложение.
- **Пропустить** – программа не выполняет никаких действий над приложением.

Специалисты «Лаборатории Касперского» рекомендуют удалять обнаруженные угрозы.

Если вредоносный объект был обнаружен во время проверки файлов, Kaspersky Internet Security по умолчанию помещает его на карантин и уведомляет вас о том, что обнаруженная угроза устранена.

Вы можете посмотреть информацию об обнаруженных вредоносных объектах в разделах **Статус** и **Отчеты**.

## КАК ЗАЩИТИТЬ ДАННЫЕ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Kaspersky Internet Security обеспечивает сохранность личных данных от несанкционированного доступа с помощью следующих способов защиты:

- Установки секретного кода, предотвращающего несанкционированный доступ к параметрам Анти-Вора и Личных контактов.
- Настройки параметров Анти-Вора.



Управление Анти-Вором осуществляется с помощью SMS-команд и команд с веб-портала <https://anti-theft.kaspersky.com>. Чтобы иметь возможность управлять функциями Анти-Вора с помощью портала, необходимо создать учетную запись на веб-портале.

Чтобы защитить ваши данные от несанкционированного доступа, необходимо зарегистрироваться на веб-портале для управления Анти-Вором, установить секретный код для ограничения доступа к параметрам программы, а также настроить устройство соответствующим образом.

## В ЭТОМ РАЗДЕЛЕ

Зачем нужен секретный код .....	<a href="#">25</a>
Что такое Kaspersky Account .....	<a href="#">25</a>
Первоначальная настройка Анти-Вора.....	<a href="#">25</a>

## ЗАЧЕМ НУЖЕН СЕКРЕТНЫЙ КОД

Секретный код программы используется в следующих случаях:

- для доступа к параметрам Анти-Вора и Личных Контактов;
- при отправке с другого мобильного устройства SMS-команды, чтобы дистанционно включить сирену на устройстве, заблокировать устройство, узнать его местоположение на карте, удалить с него данные или скрыть конфиденциальные контакты и связанную с ними информацию.

Вам предлагается установить секретный код программы при первоначальной настройке Анти-Вора (см. раздел «Первоначальная настройка Анти-Вора» на стр. [25](#)) либо при первом запуске Личных контактов. В дальнейшем вы можете изменить установленный секретный код программы.

Секретный код программы состоит из цифр. Минимальное количество символов секретного кода составляет четыре цифры.

Если вы забыли секретный код программы, вы можете восстановить его (см. раздел «Восстановление секретного кода программы» на стр. [43](#)).

## 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 Internet 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 [anti-theft.kaspersky.com](https://anti-theft.kaspersky.com), то это значит, что у вас есть Kaspersky Account.

Вы указываете учетную запись при первоначальной настройке Анти-Вора (см. раздел «Первоначальная настройка Анти-Вора» на стр. [25](#)). 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.

## ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА АНТИ-ВОРА

По умолчанию после установки программы функции Анти-Вора выключены: их невозможно запустить дистанционно с помощью веб-портала или SMS-команд. Чтобы включить функции Анти-Вора, вам нужно выполнить первоначальную настройку Анти-Вора.

После первоначальной настройки все функции Анти-Вора будут включены с параметрами, рекомендованными специалистами «Лаборатории Касперского».

Мастер первоначальной настройки Анти-Вора запускается один раз. В дальнейшем вы можете настраивать Анти-Вор в параметрах программы.

➤ *Чтобы выполнить первоначальную настройку Анти-Вора, выполните следующие действия:*

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

Запустится мастер первоначальной настройки Анти-Вора.

2. Следуйте указаниям мастера.

➤ *Чтобы изменить параметры Анти-Вора после первоначальной настройки,*

в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Анти-Вор**.

## 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 настоящий 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 полная версия Kaspersky Internet 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 функций Анти-Вора и скрытия информации на устройстве возможен, если выполнены следующие условия:

- программа Kaspersky Internet Security установлена в качестве администратора устройства;
- устройство принимает сигналы сотовой связи;
- на устройстве разрешен запуск функций Анти-Вора и скрытия информации.

➤ Чтобы дистанционно запустить функции Анти-Вора через веб-портал, 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 нужно дистанционно запустить функции Анти-Вора.
4. В блоках в верхней части окна веб-портала выберите действия, которые нужно выполнить на устройстве.

➤ Чтобы дистанционно скрыть информацию о контактах и запустить функции Анти-Вора с помощью SMS-команд, выполните одно из следующих действий:

- Сформируйте и отправьте команду на свое устройство из Kaspersky Internet Security с помощью функции отправки SMS-команды, если программа установлена на другом устройстве (см. раздел «Отправка SMS-команд из Kaspersky Internet Security» на стр. 33).

При формировании SMS-команды используйте секретный код Kaspersky Internet Security 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 (где `<код>` – это секретный код Kaspersky Internet Security, установленной на вашем устройстве);
  - `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 удаления всех данных и возврата устройства к заводским настройкам устройство не сможет получать и выполнять последующие дистанционные команды.

# РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ

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

## В ЭТОМ РАЗДЕЛЕ

---

Сканер (Антивирус) .....	<a href="#">28</a>
Личные контакты .....	<a href="#">31</a>
Анти-Вор.....	<a href="#">32</a>
Фильтр вызовов и SMS .....	<a href="#">38</a>
Веб-Фильтр и SMS Анти-Фишинг .....	<a href="#">40</a>
Другие задачи .....	<a href="#">41</a>

## СКАНЕР (АНТИВИРУС)

В бесплатной версии программы компонент называется Сканер, в полной версии – Антивирус.

Сканер (Антивирус) предназначен для проверки устройства, обнаружения и устранения угроз на вашем устройстве. Kaspersky Internet Security позволяет выполнить полную проверку содержимого устройства или частичную проверку, то есть проверить содержимое только встроенной памяти устройства или конкретной папки (в том числе и расположенной на карте памяти).

Поиск вредоносных объектов выполняется на основании антивирусных баз программы, содержащих описание всех известных в настоящий момент вредоносных программ и способов их обезвреживания, а также описания других нежелательных объектов. Крайне важно поддерживать антивирусные базы в актуальном состоянии. Рекомендуется регулярно обновлять антивирусные базы программы.

Kaspersky Internet Security выполняет обновление антивирусных баз программы с серверов обновлений «Лаборатории Касперского». Это специальные интернет-сайты, на которые выкладываются обновления баз для всех продуктов «Лаборатории Касперского».

Для обновления антивирусных баз программы на устройстве должно быть настроено соединение с интернетом. Трафик при обновлении антивирусных баз программы оплачивается согласно вашему тарифному плану.

**В ЭТОМ РАЗДЕЛЕ**

Полная проверка устройства.....	<a href="#">29</a>
Быстрая проверка .....	<a href="#">29</a>
Проверка папок и файлов.....	<a href="#">29</a>
Автоматическая проверка по расписанию.....	<a href="#">30</a>
Обновление антивирусных баз и версий программы .....	<a href="#">30</a>
Автоматическое обновление по расписанию.....	<a href="#">30</a>

**ПОЛНАЯ ПРОВЕРКА УСТРОЙСТВА**

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,*

в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Проверка > Полная проверка**.

**БЫСТРАЯ ПРОВЕРКА**

С помощью быстрой проверки вы можете проверить только установленные программы.

Если вы используете бесплатную версию, «Лаборатория Касперского» рекомендует запускать быструю проверку после установки новых программ.

♦ *Чтобы выполнить быструю проверку,*

в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Проверка > Быстрая проверка**.

**ПРОВЕРКА ПАПОК И ФАЙЛОВ**

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

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

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Проверка > Проверка папки**.
2. Выберите папку или файл для проверки.

## АВТОМАТИЧЕСКАЯ ПРОВЕРКА ПО РАСПИСАНИЮ

Вы можете настроить автоматический запуск полной проверки устройства и создать расписание запуска проверки: 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 Internet Security в панели быстрого запуска нажмите **Настройка > Антивирус > Параметры проверки**.
2. Настройте периодичность запуска проверки. Для этого выберите значение для параметра **Расписание**.
3. Настройте день и время запуска проверки. Для этого выберите значения для параметров **День запуска** и **Время запуска**.

Проверка будет запускаться согласно расписанию.

## ОБНОВЛЕНИЕ АНТИВИРУСНЫХ БАЗ И ВЕРСИЙ ПРОГРАММЫ

Kaspersky Internet 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. Рекомендуется регулярно обновлять антивирусные базы.

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

Для обновления антивирусных баз программы на устройстве должно быть настроено соединение с интернетом.

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

➔ *Чтобы обновить антивирусные базы и версию программы,*

в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Обновление**.

## АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ ПО РАСПИСАНИЮ

Вы можете настроить автоматический запуск обновления антивирусных баз и версии программы (далее «обновление»). Для этого вы можете создать расписание обновления: 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 полной версии Kaspersky Internet 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 Internet Security в панели быстрого запуска нажмите **Настройка > Антивирус > Обновление**.
  2. Настройте 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**.
- Обновление будет запускаться согласно расписанию.

## ЛИЧНЫЕ КОНТАКТЫ

Вы можете скрывать ваши конфиденциальные контакты, а также историю разговоров и SMS-переписку с этими контактами с помощью компонента Личные контакты.

Личные контакты доступны только в полной версии Kaspersky Internet Security.

Личные контакты позволяют выполнять следующие действия:

- формировать список скрываемых контактов, в котором перечислены конфиденциальные номера;
- скрывать информацию о контактах в телефонной книге, в прочитанных входящих SMS, переданных и черновиках SMS, а также записи о контактах в журнале вызовов;
- блокировать сигналы о получении SMS и входящие вызовы с конфиденциальных номеров (звонящий в этом случае получает сигнал «Занято»).

Чтобы посмотреть вызовы и SMS, поступившие в тот период, когда скрытие конфиденциальной информации было включено, требуется отключить скрытие информации. Если вы повторно включаете скрытие информации, конфиденциальная информация снова становится скрытой.

Вы можете включить скрытие информации в программе или дистанционно с помощью SMS-команды, отправленной с другого мобильного устройства. Вы можете отправить стандартное SMS со специальным текстом или отправить SMS из Kaspersky Internet 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.

Доступ к управлению Личными контактами защищен секретным кодом (см. раздел «Зачем нужен секретный код» на стр. 25). Секретный код устанавливается при первоначальной настройке Анти-Вора (см. раздел «Первоначальная настройка Анти-Вора» на стр. 25) либо при первом открытии Личных контактов.

### В ЭТОМ РАЗДЕЛЕ

Скрытие информации для контактов .....	<a href="#">32</a>
Дистанционный запуск скрытия с другого устройства .....	<a href="#">32</a>

## СКРЫТИЕ ИНФОРМАЦИИ ДЛЯ КОНТАКТОВ

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

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Личные контакты**.

2. Введите секретный код программы.

Если вы забыли секретный код, вы можете его восстановить (см. раздел «Восстановление секретного кода программы» на стр. 43).

3. Нажмите **Скрываемые контакты**.

4. Нажмите **Добавить**, чтобы сформировать список скрываемых контактов.

В списке содержатся контакты, о которых вы хотите скрывать информацию. Если список контактов сформирован, пропустите этот шаг.

5. Установите переключатель **Личные контакты** в состояние **включено**.

## ДИСТАНЦИОННЫЙ ЗАПУСК СКРЫТИЯ С ДРУГОГО УСТРОЙСТВА

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

Дистанционный запуск функции скрытия информации возможен, если выполнены следующие условия:

- на устройстве, принимающем SMS-команду, активирована полная версия программы;
- устройство принимает сигналы сотовой связи;
- на устройстве разрешен дистанционный запуск функции скрытия информации.

► Чтобы дистанционно скрыть информацию на своем устройстве, выполните одно из следующих действий:

- На другом устройстве сформируйте и отправьте команду на ваше устройство из Kaspersky Internet Security с помощью функции отправки SMS-команды (если программа установлена на другом устройстве).
- На другом устройстве создайте и отправьте на ваше устройство SMS со специальным текстом `hide:<код>` (где `<код>` – это секретный код Kaspersky Internet Security на вашем устройстве).

Отчет о выполнении команды вы получите в ответном SMS.

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

## АНТИ-ВОР

Анти-Вор защищает вашу информацию на устройстве от несанкционированного доступа и помогает найти устройство в случае его кражи или потери.

С помощью веб-портала <https://anti-theft.kaspersky.com> или специальных SMS-команд вы можете дистанционно выполнить следующие действия:

- заблокировать устройство и определить его местоположение;



- включить на устройстве громкую сирену;
- удалить данные с устройства;
- получить фотографии человека, который использует устройство.

Также в случае замены SIM-карты на устройстве или включения устройства без нее, вы можете дистанционно заблокировать устройство и узнать новый номер телефона. Это позволит вам запустить другие функции Анти-Вора на утерянном устройстве.

## В ЭТОМ РАЗДЕЛЕ

Добавление устройства в учетную запись на веб-портале.....	<a href="#">33</a>
Отправка SMS-команд из Kaspersky Internet Security .....	<a href="#">33</a>
Дистанционный контроль SIM-карты .....	<a href="#">34</a>
Дистанционное блокирование и поиск устройства .....	<a href="#">34</a>
Дистанционное включение сирены на устройстве.....	<a href="#">35</a>
Дистанционное удаление данных с устройства.....	<a href="#">36</a>
Дистанционное фотографирование.....	<a href="#">37</a>

## ДОБАВЛЕНИЕ УСТРОЙСТВА В УЧЕТНУЮ ЗАПИСЬ НА ВЕБ-ПОРТАЛЕ

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

Чтобы добавить устройство к вашей учетной записи, во время первоначальной настройки Kaspersky Internet 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.

## ОТПРАВКА SMS-КОМАНД ИЗ KASPERSKY INTERNET 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 установлен Kaspersky Internet Security, вы можете отправить SMS-команду из программы. Для отправки SMS-команды требуется знать секретный код Kaspersky Internet Security на вашем устройстве.

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

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

1. Откройте на другом устройстве Kaspersky Internet Security.
2. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Анти-Вор**.

3. Введите секретный код программы.
4. Если вы забыли секретный код, вы можете его восстановить (см. раздел «Восстановление секретного кода программы» на стр. [43](#)).
5. Нажмите **Отправка SMS-команд**.
6. Нажмите **Отправить SMS-команду**, затем сформируйте и отправьте команду на ваше устройство. При формировании SMS-команды используйте секретный код Kaspersky Internet Security на вашем устройстве.

Отчет о выполнении команды вы получите в ответном SMS.

## ДИСТАНЦИОННЫЙ КОНТРОЛЬ SIM-КАРТЫ

В случае замены SIM-карты на устройстве или включения устройства без нее, вы можете дистанционно заблокировать устройство и узнать новый номер телефона. Это позволит вам запустить другие функции Анти-Вора на утерянном устройстве.

Вы можете получить новый номер телефона по SMS или по электронной почте. Если функция включена, при включении утерянного устройства без SIM-карты программа автоматически блокирует устройство. При замене SIM-карты в устройстве программа автоматически посылает SMS и письмо с новым номером телефона на указанные вами номер телефона и адрес электронной почты.

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. Оплата за отправку SMS на специальный номер списываются с мобильного счета, соответствующего новой установленной SIM-карте.

➤ *Чтобы включить контроль SIM-карты, предварительно выполните следующие действия:*

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Анти-Вор**.
2. Введите секретный код программы.
3. Если вы забыли секретный код, вы можете его восстановить (см. раздел «Восстановление секретного кода программы» на стр. [43](#)).
4. Установите флажок **SIM-Контроль**.
5. 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.
6. В блоке **Параметры блокирования** установите флажок **Блокировать при смене SIM-карты**, чтобы заблокировать устройство при замене SIM-карты или включении без нее.

Если требуется, в поле **Текст при блокировании** введите текст сообщения, которое будет отображаться на экране заблокированного устройства.

## ДИСТАНЦИОННОЕ БЛОКИРОВАНИЕ И ПОИСК УСТРОЙСТВА

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 Internet Security на вашем устройстве).

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

Дистанционное блокирование и определение местоположения устройства возможны, если выполнены следующие условия:

- Kaspersky Internet Security установлен в качестве администратора устройства;
- устройство принимает сигналы сотовой связи;
- запуск этой функции разрешен на устройстве.

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

► *Чтобы заблокировать свое устройство и получить координаты его местоположения на карте через веб-портал, 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, 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**.

Когда Kaspersky Internet 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 Internet Security с помощью функции отправки SMS-команды, если программа установлена на другом устройстве (см. раздел «Отправка SMS-команд из Kaspersky Internet Security» на стр. 33). При формировании SMS-команды используйте секретный код Kaspersky Internet Security на вашем устройстве.
- Отправьте SMS на ваше устройство со следующим специальным текстом `find: <код>` (где <код> – это секретный код Kaspersky Internet Security на вашем устройстве).

Когда Kaspersky Internet Security обнаружит ваше устройство, вы получите его координаты в ответном SMS, а также на указанный адрес электронной почты.

## ДИСТАНЦИОННОЕ ВКЛЮЧЕНИЕ СИРЕНЫ 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 Internet Security на вашем устройстве).

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

Дистанционное включение сирены возможно, если устройство принимает сигналы сотовой связи и запуск этой функции разрешен на устройстве.

➤ Чтобы включить сирену на устройстве и заблокировать его через веб-портал, 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, 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**.

➤ 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 Internet Security с помощью функции отправки SMS-команды, если программа установлена на другом устройстве (см. раздел «Отправка SMS-команд из Kaspersky Internet Security» на стр. 33). При формировании SMS-команды используйте секретный код Kaspersky Internet Security на вашем устройстве.
- Отправьте SMS на ваше устройство со следующим специальным текстом `alarm: <код>` (где <код> – это секретный код Kaspersky Internet Security на вашем устройстве).

Отчет о выполнении команды вы получите в ответном SMS.

## ДИСТАНЦИОННОЕ УДАЛЕНИЕ ДАННЫХ С УСТРОЙСТВА

При краже или потере вашего устройства вы можете дистанционно удалить данные с устройства с помощью веб-портала <https://anti-theft.kaspersky.com> или SMS-команд.

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 (вернуть устройство к заводским настройкам).

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

Дистанционное удаление данных возможно, если выполнены следующие условия:

- Kaspersky Internet Security установлен в качестве администратора устройства;
- устройство принимает сигналы сотовой связи;

- запуск этой функции разрешен на устройстве.

➤ Чтобы дистанционно удалить данные с устройства через веб-портал, 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, 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 Internet Security также будет удалена. Устройство не сможет больше выполнять дистанционные команды.

6. Нажмите на кнопку **Удалить**.

➤ 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 Internet Security с помощью функции отправки SMS-команды, если программа установлена на другом устройстве (см. раздел «Отправка SMS-команд из Kaspersky Internet Security» на стр. 33). Вы можете выбрать удаление персональных данных или всех данных. При формировании SMS-команды используйте секретный код Kaspersky Internet Security 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 Internet Security на вашем устройстве.

Отчет о выполнении команды вы получите в ответном SMS.

## ДИСТАНЦИОННОЕ ФОТОГРАФИРОВАНИЕ

При краже или потере устройства вы можете дистанционно получить фотографии человека, который использует устройство, и заблокировать устройство с помощью веб-портала <https://anti-theft.kaspersky.com>.

Дистанционное фотографирование доступно, если ваше устройство оборудовано фронтальной камерой. Включение функции возможно только через веб-портал. Включение с помощью SMS-команды не поддерживается.

Дистанционный запуск функции Анти-Вора возможен, если выполнены следующие условия:

- программа Kaspersky Internet Security установлена в качестве администратора устройства;
- устройство принимает сигналы сотовой связи;
- 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 Kaspersky Account, 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**.

Когда Kaspersky Internet Security выполнит команду, фотографии будут доступны на веб-портале. После получения фотографий вы можете отправить команду повторно.

## ФИЛЬТР ВЫЗОВОВ И SMS

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

Фильтр вызовов и SMS позволяет вам блокировать нежелательные входящие вызовы и SMS. Программа фильтрует вызовы и SMS на основе списков разрешенных и запрещенных контактов и в соответствии с выбранным режимом фильтрации.

### В ЭТОМ РАЗДЕЛЕ

Стандартная фильтрация контактов.....	<a href="#">38</a>
Блокирование всех контактов, кроме разрешенных.....	<a href="#">39</a>
Блокирование только запрещенных контактов .....	<a href="#">39</a>

## СТАНДАРТНАЯ ФИЛЬТРАЦИЯ КОНТАКТОВ

Если вы хотите получать вызовы и SMS от разрешенных контактов, и блокировать – от запрещенных контактов, используйте стандартный режим фильтрации.

Если вам позвонит или придет SMS контакт, которого нет в разрешенном и запрещенном списках, программа предложит вам выбрать действие над вызовом или SMS от этого контакта. В дальнейшем программа будет автоматически обрабатывать вызовы и SMS от этого контакта в соответствии с вашим выбором.

➤ Чтобы включить стандартный режим фильтрации, выполните следующие действия:

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Фильтр вызовов и SMS > Режим Фильтра вызовов и SMS > Стандартный**.
2. Сформируйте список запрещенных контактов. Для этого в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Фильтр вызовов и SMS > Запрещенные контакты**.
3. Сформируйте список разрешенных контактов. Для этого в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Фильтр вызовов и SMS > Разрешенные контакты**.
4. Если требуется, включите дополнительные параметры фильтрации. Для этого в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройки > Фильтр вызовов и SMS**.

Чтобы разрешить прием вызовов и SMS от всех контактов из телефонной книги устройства, установите флажок **Разрешать Контакты**.

Чтобы запретить прием SMS с номеров, содержащих буквы, установите флажок **Блокировать нечисловые номера**.

## БЛОКИРОВАНИЕ ВСЕХ КОНТАКТОВ, КРОМЕ РАЗРЕШЕННЫХ

Если вы хотите блокировать вызовы и SMS от всех контактов кроме разрешенных, используйте фильтрацию в режиме разрешенных контактов.

➤ Чтобы включить фильтрацию в режиме разрешенных контактов, выполните следующие действия:

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Фильтр вызовов и SMS > Режим Фильтра вызовов и SMS > Разрешенные контакты**.
2. Сформируйте список разрешенных контактов. Для этого в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Фильтр вызовов и SMS > Разрешенные контакты**.
3. Если требуется, разрешите прием вызовов и SMS от контактов из телефонной книги устройства:
  - a. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройки > Фильтр вызовов и SMS**.
  - b. Установите флажок **Разрешать Контакты**.

## БЛОКИРОВАНИЕ ТОЛЬКО ЗАПРЕЩЕННЫХ КОНТАКТОВ

Если вы хотите блокировать вызовы и SMS только от запрещенных контактов, используйте фильтрацию в режиме запрещенных контактов.

➤ Чтобы включить фильтрацию в режиме запрещенных контактов, выполните следующие действия:

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Фильтр вызовов и SMS > Режим Фильтра вызовов и SMS > Запрещенные контакты**.
2. Сформируйте список запрещенных контактов. Для этого в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Фильтр вызовов и SMS > Запрещенные контакты**.
3. Если требуется, включите автоматическую блокировку SMS с номеров, содержащих буквы:
  - a. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройки > Фильтр вызовов и SMS**.
  - b. Установите флажок **Блокировать нечисловые номера**.

## ВЕБ-ФИЛЬТР И SMS АНТИ-ФИШИНГ

С Веб-Фильтром и SMS Анти-Фишингом вы можете посещать проверенные веб-сайты и безопасно работать с персональными данными в сети.

Веб-Фильтр и SMS Анти-Фишинг доступны только в полной версии Kaspersky Internet Security.

SMS Анти-Фишинг доступен только на устройствах с установленной SIM-картой.

Веб-Фильтр блокирует вредоносные веб-сайты, цель которых – распространить вредоносный код, а также поддельные (фишинговые) веб-сайты, цель которых – украсть ваши конфиденциальные данные 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 до их открытия. SMS Анти-Фишинг проверяет ссылки в SMS также до их открытия. Для проверки Веб-Фильтр и SMS Анти-Фишинг используют облачный сервис Kaspersky Security Network (специальный онлайн-сервис «Лаборатории Касперского», который содержит информацию о надежности файлов, программ и интернет-ресурсов).

### В ЭТОМ РАЗДЕЛЕ

Постоянная проверка веб-сайтов..... [40](#)

Постоянная проверка ссылок в SMS..... [40](#)

## ПОСТОЯННАЯ ПРОВЕРКА ВЕБ-САЙТОВ

Веб-Фильтр проверяет веб-сайты только в стандартном браузере Android и не проверяет их в других браузерах. Если вы хотите постоянно использовать Веб-Фильтр при работе в интернете, выберите стандартный браузер Android в качестве браузера по умолчанию.

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

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Веб-Фильтр**.
2. Установите переключатель **Веб-Фильтр** в положение **включен**.
3. Нажмите **Изменить браузер** (кнопка отображается, если Веб-Фильтр включен, и браузером по умолчанию является не стандартный браузер Android).  
Будет запущен мастер выбора браузера по умолчанию.
4. Следуйте указаниям мастера.

В результате работы мастера стандартный браузер Android будет использоваться как браузер по умолчанию.

## ПОСТОЯННАЯ ПРОВЕРКА ССЫЛОК В SMS

SMS Анти-Фишинг доступен только на устройствах с установленной SIM-картой.



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

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Веб-Фильтр**.
2. Установите переключатель **SMS Анти-Фишинг** в положение **включен**.

## ДРУГИЕ ЗАДАЧИ

Дополнительно вы можете выполнить следующие операции:

- активировать полную версию программы;
- приобрести лицензию или продлить срок ее действия;
- просмотреть информацию о лицензии;
- просмотреть отчеты о работе программы (например, отчеты о выполненной проверке, о найденных угрозах, о заблокированных SMS, вызовах или веб-сайтах);
- изменить секретный код программы;
- восстановить секретный код программы.

### В ЭТОМ РАЗДЕЛЕ

Приобретение лицензии и продление срока ее действия.....	<a href="#">41</a>
Активация полной версии программы .....	<a href="#">42</a>
Просмотр информации о лицензии, сроке ее действия .....	<a href="#">42</a>
Просмотр отчетов о работе программы .....	<a href="#">42</a>
Изменение секретного кода программы .....	<a href="#">43</a>
Восстановление секретного кода программы .....	<a href="#">43</a>

## ПРИБРЕТЕНИЕ ЛИЦЕНЗИИ И ПРОДЛЕНИЕ СРОКА ЕЕ ДЕЙСТВИЯ

Если вы решили использовать полную версию Kaspersky Internet Security, вы можете приобрести лицензию на использование программы в интернет-магазине «Лаборатории Касперского» или компаний-партнеров. При приобретении лицензии вы получите код активации, с помощью которого вам нужно активировать полную версию программы.

Когда срок действия лицензии подходит к концу, вы можете его продлить. Для этого вы можете либо приобрести новую лицензию в интернет-магазине, либо использовать код активации (см. раздел «О коде активации» на стр. [22](#)) для лицензии, приобретенной заранее.

По истечении срока действия лицензии программа автоматически переходит на бесплатную версию.

➤ Чтобы приобрести лицензию в интернет-магазине, выполните следующие действия:

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Дополнительные настройки > Лицензирование**.
2. Выберите **Приобретение лицензии**.

3. Нажмите **Открыть**.

Откроется веб-страница интернет-магазина, где вы можете приобрести новую лицензию.

➤ *Чтобы продлить срок действия лицензии с помощью кода активации, выполните следующие действия:*

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Дополнительные настройки > Лицензирование**.
2. Выберите **Ввод кода активации**.
3. Введите код активации для лицензии, приобретенной заранее.

## АКТИВАЦИЯ ПОЛНОЙ ВЕРСИИ ПРОГРАММЫ

Чтобы использовать все функции программы, вам нужно активировать полную версию Kaspersky Internet Security.

*Активация* – это перевод программы в полнофункциональный режим. Для активации вам необходимо ввести код активации, который вы получили при приобретении лицензии, либо приобрести лицензию в интернет-магазине.

Вы можете активировать полную версию программы при первом запуске или в любое время позже.

Чтобы активировать полную версию, вам нужно ввести код активации (см. раздел «О коде активации» на стр. [22](#)), который вы получили при приобретении лицензии, либо приобрести лицензию в интернет-магазине (см. раздел «Приобретение лицензии и продление срока ее действия» на стр. [41](#)).

Для активации программы нужно активное интернет-соединение.

➤ *Чтобы активировать полную версию программы с помощью кода активации, выполните следующие действия:*

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Дополнительные настройки > 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.

## ПРОСМОТР ИНФОРМАЦИИ О ЛИЦЕНЗИИ, СРОКЕ ЕЕ ДЕЙСТВИЯ

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

*Информация о лицензии доступна для просмотра, если вы используете пробную версию или полную версию программы.*

➤ *Чтобы проверить срок действия лицензии и просмотреть информацию о лицензии,*

в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Лицензирование > Подробнее о лицензии**.

## ПРОСМОТР ОТЧЕТОВ О РАБОТЕ ПРОГРАММЫ

События, которые происходят в ходе работы Сканера (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,*

в главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Отчеты**.

## ИЗМЕНЕНИЕ СЕКРЕТНОГО КОДА ПРОГРАММЫ

Программа предлагает установить секретный код при первоначальной настройке Анти-Вора (см. раздел «Первоначальная настройка Анти-Вора» на стр. 25) либо при первом запуске Личных контактов. Вы можете изменить секретный код в любое время.

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

1. В главном окне Kaspersky Internet Security в панели быстрого запуска нажмите **Настройка > Дополнительные настройки > 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 новый код еще раз в поле **Повторно введите новый код** и нажмите **Вход**.

## ВОССТАНОВЛЕНИЕ СЕКРЕТНОГО КОДА 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 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.

# 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 .....	44
Техническая поддержка по телефону .....	44
Получение технической поддержки через Личный кабинет .....	44

## 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 лицензию на использование программы. Техническая поддержка для пользователей пробных версий не осуществляется.

## ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ПО ТЕЛЕФОНУ

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

Перед обращением в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами предоставления поддержки <http://support.kaspersky.ru/support/rules>. 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 Internet 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 Internet 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 Internet 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 ввести код активации, полученный при приобретении лицензии, либо приобрести лицензию в интернет-магазине.

### **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

### **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 лицензию на использование Kaspersky Internet 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.

**С****СЕКРЕТНЫЙ КОД ПРОГРАММЫ**

Секретный код программы используется в следующих случаях:

- для доступа к параметрам Анти-Вора и Личных Контактов;
- при отправке с другого мобильного устройства SMS-команды, чтобы дистанционно включить сирену на устройстве, заблокировать устройство, узнать его местоположение на карте, удалить с него данные или скрыть конфиденциальные контакты и связанную с ними информацию.

**СПИСОК ЗАПРЕЩЕННЫХ КОНТАКТОВ**

В список запрещенных контактов вы можете внести те контакты, от которых вы не хотите получать входящие события.

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.

**СПИСОК РАЗРЕШЕННЫХ КОНТАКТОВ**

В список разрешенных контактов вы можете внести те контакты, от которых вы хотите получать входящие события.

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.

**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/>

Вирусная 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 .....25

## А

Активация программы .....42  
код активации.....42  
купить код активации онлайн.....41  
лицензия.....21  
Анти-Вор.....26, 33, 34, 35, 36, 37  
SIM-Контроль .....34  
Блокирование и Поиск.....26, 34  
Сирена.....35  
Тайное фото.....37  
Удаление данных.....26, 36

## В

Виджет главного экрана.....19

## Г

Главное окно программы .....15

## З

Запуск  
обновление вручную.....30  
проверка устройства вручную.....29  
проверка устройства по расписанию.....30  
программа .....23  
Значок в строке состояния.....18

## К

Код  
восстановить секретный код.....43  
изменить секретный код программы .....43

## Л

Лицензионное соглашение .....21  
Лицензия  
активация программы.....42  
информация .....42  
Лицензионное соглашение.....21, 41, 42  
продление .....41  
продлить онлайн.....41  
Личные контакты .....32  
дистанционный запуск.....32

## О

Обновление  
запуск вручную.....30  
запуск по расписанию.....30  
точка доступа .....30  
Определение местоположения устройства.....26, 34  
Отправка SMS-команды.....26, 32, 33  
Отчеты.....42

**П**

Проверка по требованию .....29, 30  
Продление срока действия лицензии .....41

**Р**

Расписание  
    Обновление .....30  
    Проверка по требованию .....30

**С**

Секретный код программы .....43  
Сирена .....35

**У**

Уведомления программы .....19