

Kaspersky Internet Security для Mac

KASPERSKY для

Руководство пользователя

ВЕРСИЯ ПРОГРАММЫ: 14.0 MAINTENANCE RELEASE 1

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: 25.09.2013

© ЗАО «Лаборатория Касперского», 2013

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

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ	6
В этом документе	6
Условные обозначения	8
ИСТОЧНИКИ ИНФОРМАЦИИ О ПРОГРАММЕ	9
Источники информации для самостоятельного поиска	9
Обсуждение программ «Лаборатории Касперского» на форуме	10
Обращение в Департамент продаж	10
Обращение в Отдел локализации и разработки технической документации	10
KASPERSKY INTERNET SECURITY	11
Комплект поставки	12
Сервис для пользователей	13
Аппаратные и программные требования	13
УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ	14
Подготовка к установке программы	14
Процедура установки программы	14
Загрузка программы с последующей установкой с веб-сайта Kaspersky Protection Center	15
О Kaspersky Account	15
О веб-сайте Kaspersky Protection Center	16
Установка программы с установочного диска или дистрибутива	16
Подготовка программы к работе	17
Удаление программы	18
ИНТЕРФЕЙС ПРОГРАММЫ	19
Значок Kaspersky Internet Security	19
Главное окно программы	20
Окно настройки программы	21
Окно настройки Родительского контроля	22
Окна уведомлений и всплывающие сообщения	23
Об окнах уведомлений	23
О типах событий	23
О всплывающих сообщениях	23
Выключение доставки уведомлений	24
Новостной агент	24
ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ	25
О Лицензионном соглашении	25
О лицензии	25
О подписке	26
О коде активации	27
О предоставлении данных	27
Просмотр информации о лицензии	29
Приобретение лицензии	29
Продление срока действия лицензии	30
Продление подписки	30
Обновление статуса подписки	30
Активация Kaspersky Internet Security	31

Активация пробной версии программы	31
Активация программы с помощью кода активации	32
ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ	34
СОСТОЯНИЕ ЗАЩИТЫ КОМПЬЮТЕРА.....	35
Оценка состояния защиты компьютера	35
Выключение защиты компьютера.....	36
Возобновление защиты компьютера.....	37
Использование Центра защиты	37
РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ	39
Как выполнить полную проверку компьютера на вирусы	39
Как выполнить быструю проверку компьютера	40
Как проверить на вирусы файл, папку или диск	40
Как приобрести лицензию	40
Как продлить срок действия лицензии	41
Как обновить базы программы.....	41
Как защитить от перехвата данные, вводимые с клавиатуры.....	41
Как ограничить время работы пользователя в интернете.....	42
Как ограничить посещение веб-сайтов и загрузку файлов из интернета	43
Как ограничить контакты и переписку пользователя в социальных сетях	43
Как запретить пересылку персональных данных	44
Что делать, если программа заблокировала доступ к файлу	44
Как восстановить удаленный или вылеченный программой объект.....	45
Как просмотреть отчет о работе программы	46
Что делать при появлении окон уведомлений и всплывающих сообщений	46
РАБОТА С ПРОГРАММОЙ ИЗ КОМАНДНОЙ СТРОКИ.....	47
Просмотр справки	48
Проверка на вирусы.....	48
Обновление программы	50
Откат последнего обновления	51
Запуск / остановка работы компонента или задачи	51
Статистика работы компонента или задачи	52
Экспорт параметров защиты	53
Импорт параметров защиты	53
Активация программы	53
Завершение работы программы.....	54
Коды возврата командной строки.....	54
ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ.....	55
Способы получения технической поддержки	55
Техническая поддержка по телефону	55
Получение технической поддержки через Личный кабинет	56
Использование файла трассировки	57
Создание файла трассировки.....	57

ГЛОССАРИЙ.....	58
ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»	60
ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ	61
УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ	62
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ	63

ОБ ЭТОМ РУКОВОДСТВЕ

Этот документ представляет собой Руководство пользователя Kaspersky Internet Security для Mac.

Для успешного использования Kaspersky Internet Security пользователям нужно быть знакомыми с интерфейсом операционной системы Mac OS X, владеть основными приемами работы в ней, уметь работать с электронной почтой и интернетом.

Руководство предназначено для следующих целей:

- Помочь установить Kaspersky Internet Security, активировать и использовать программу.
- Обеспечить быстрый поиск информации для решения 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 [6](#)

Условные обозначения [8](#)

В ЭТОМ ДОКУМЕНТЕ

В Руководство пользователя Kaspersky Internet Security включены следующие разделы:

Источники информации о программе (см. стр. [9](#))

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

Kaspersky Internet Security (см. стр. [11](#))

Этот раздел содержит описание возможностей программы, а также краткую информацию о ее компонентах и основных функциях. Из раздела вы узнаете о комплектах поставки и о комплексе услуг, доступных зарегистрированным пользователям программы. В разделе приведены аппаратные и программные требования, которым должен отвечать компьютер, чтобы на него можно было установить Kaspersky Internet Security.

Установка и удаление программы (см. стр. [14](#))

Этот раздел содержит пошаговые инструкции по установке и удалению программы.

Интерфейс программы (см. стр. [19](#))

Этот раздел содержит описание основных элементов графического интерфейса Kaspersky Internet Security: значка программы и контекстного меню значка программы, главного окна и окна настройки программы, окна Родительского контроля. Также раздел содержит информацию об окнах уведомлений и всплывающих сообщениях программы.

Лицензирование программы (см. стр. [25](#))

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 (см. стр. [34](#))

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

Состояние защиты компьютера (см. стр. [35](#))

Этот раздел содержит информацию о том, как определить наличие проблем и угроз безопасности компьютера и настроить уровень его защиты. Из этого раздела вы также узнаете о включении и отключении защиты во время работы программы.

Решение типовых задач (см. стр. [39](#))

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

Работа с программой из командной строки (см. стр. [47](#))

Этот раздел содержит подробное описание работы с программой и ее компонентами с использованием командной строки.

Обращение в Службу технической поддержки (см. стр. [55](#))

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

Глоссарий

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

ЗАО «Лаборатория Касперского» (см. стр. [60](#))

Этот раздел содержит информацию о ЗАО «Лаборатория Касперского».

Информация о стороннем коде (см. стр. [61](#))

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

Уведомления о товарных знаках (см. стр. [62](#))

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, что...	Предупреждения выделены красным цветом и заключены в рамку. В предупреждениях содержится информация о возможных нежелательных действиях, которые могут привести к потере информации, сбоям в работе оборудования или операционной системы.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания могут содержать полезные советы, рекомендации, особые значения параметров или важные частные случаи в работе программы.
Пример: ...	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"> • новые термины; • названия статусов и событий программы.
Command-A	Названия клавиш клавиатуры выделены полужирным шрифтом. Названия клавиш, соединенные знаком «минус», означают комбинацию клавиш.
Нажмите на кнопку Включить .	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».
kav update	Специальным стилем выделены следующие типы текста: <ul style="list-style-type: none"> • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести пользователю.
<IP-адрес вашего компьютера>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

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.....	9
Обсуждение программ «Лаборатории Касперского» на форуме.....	10
Обращение в Департамент продаж.....	10
Обращение в Отдел локализации и разработки технической документации.....	10

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.

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. [55](#)). 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/mac-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/kismac>) 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.

Для перехода к Базе знаний откройте главное окно программы (на стр. [20](#)), нажмите на кнопку  и в открывшемся окне нажмите на кнопку **Служба технической поддержки**.

Электронная справка

В состав электронной справки программы входят файлы контекстной справки.

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

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.

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 [электронному адресу](#). В качестве темы письма нужно указать «Kaspersky Help Feedback: Kaspersky Internet Security для Mac».

KASPERSKY INTERNET SECURITY

Kaspersky Internet Security для Mac предназначен для защиты компьютеров, работающих под управлением операционной системы Mac OS X, от воздействия вирусов и других программ, представляющих угрозу.

В состав программы входят следующие компоненты:

Файловый Антивирус

Компонент защищает файловую систему компьютера в режиме реального времени: перехватывает и анализирует обращения к файловой системе, лечит, удаляет зараженные и изолирует возможно зараженные объекты для дальнейшего анализа.

Веб-Антивирус и антифишинг

Компонент обеспечивает защиту информации, поступающей на ваш компьютер и отправляющейся с него по протоколам HTTP и HTTPS. Проверка ссылок на веб-страницах на наличие фишинга и на принадлежность к вредоносным веб-адресам с помощью модуля проверки ссылок. Предотвращение перехвата персональных данных, вводимых с клавиатуры, с помощью виртуальной клавиатуры.

Родительский контроль

Компонент обеспечивает контроль действий разных пользователей на компьютере и в интернете. Компонент позволяет ограничивать доступ в интернет по времени и доступ к интернет-ресурсам и программам, создавать списки контактов, запрещенных или разрешенных для общения в социальных сетях, контролировать пересылку определенных персональных данных. Также компонент позволяет просматривать отчеты о действиях и активности пользователей.

В программе реализованы следующие функции:

Поиск вирусов

Поиск и обезвреживание вирусов и других программ, представляющих угрозу, по запросу пользователя: поиск и анализ зараженных и возможно зараженных объектов в заданных областях проверки, лечение, удаление или изоляция объектов для дальнейшего анализа.

В состав Kaspersky Internet Security включены наиболее востребованные пользователями задачи поиска вирусов: полная проверка всех объектов компьютера и быстрая проверка важных областей.

Обновление

Обновление антивирусных баз Kaspersky Internet Security с серверов обновлений «Лаборатории Касперского», создание резервной копии всех обновляемых файлов на случай необходимости отката последнего произведенного обновления. Также программа позволяет загружать и устанавливать новые версии Kaspersky Internet Security в автоматическом режиме.

Карантин

Создание копии зараженного объекта в хранилище карантина перед лечением и удалением в целях возможного восстановления объекта, представляющего информационную ценность.

Отчеты

Формирование подробного отчета о работе каждого компонента Kaspersky Internet Security.

Уведомления

Уведомление пользователя о возникновении определенных событий в работе Kaspersky Internet Security с помощью окон уведомлений и всплывающих сообщений, которые могут дополняться звуковым оповещением.

Во время работы Kaspersky Internet Security выводит сообщения о состоянии защиты. Центр защиты (см. раздел «Использование Центра защиты» на стр. 37), включенный в состав программы, позволяет получить полную картину текущего состояния защиты компьютера и перейти к немедленному устранению проблем и угроз безопасности.

В ЭТОМ РАЗДЕЛЕ

Комплект поставки.....	12
Сервис для пользователей.....	13
Аппаратные и программные требования.....	13

КОМПЛЕКТ ПОСТАВКИ

Вы можете приобрести программу одним из следующих способов:

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

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

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

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

Если вы приобретаете Kaspersky 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.

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.

АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ

Для функционирования Kaspersky Internet Security компьютер должен удовлетворять следующим требованиям:

- операционная система Mac OS X 10.6, 10.7, OS X 10.8, 10.9;
- 350 МБ свободного места на жестком диске (в зависимости от размера антивирусных баз).

УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ

Этот раздел содержит пошаговые инструкции по установке и удалению программы.

В состав дистрибутива Kaspersky Internet Security входят программа установки и программа удаления Kaspersky Internet Security.

В ЭТОМ РАЗДЕЛЕ

Подготовка к установке программы	14
Процедура установки программы	14
Подготовка программы к работе	17
Удаление программы	18

ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММЫ

Перед установкой Kaspersky Internet Security на компьютер рекомендуется выполнить ряд подготовительных действий:

- Убедиться, что ваш компьютер соответствует аппаратным и программным требованиям (см. раздел «Аппаратные и программные требования» на стр. [13](#)).
- Проверить подключение компьютера к интернету. Доступ в интернет требуется для входа на веб-сайт Kaspersky Protection Center (см. раздел «О веб-сайте Kaspersky Protection Center» на стр. [16](#)) с помощью Kaspersky Account (см. раздел «О Kaspersky Account» на стр. [15](#)), загрузки новой версии Kaspersky Internet Security на компьютер, активации программы с помощью кода активации, а также для получения обновлений.
- Удалить с компьютера другие антивирусные программы, чтобы избежать возникновения системных конфликтов и снижения быстродействия операционной системы.

ПРОЦЕДУРА УСТАНОВКИ ПРОГРАММЫ

Существуют следующие способы установки Kaspersky Internet Security на компьютер:

- Загрузка с последующей установкой с веб-сайта Kaspersky Protection Center с помощью Kaspersky Account (см. раздел «Загрузка программы с последующей установкой с веб-сайта Kaspersky Protection Center» на стр. [15](#)).

Выполняется с помощью Kaspersky Account (см. раздел «О Kaspersky Account» на стр. [15](#)). Позволяет загрузить с веб-сайта Kaspersky Protection Center (см. раздел «О веб-сайте Kaspersky Protection Center» на стр. [16](#)) и установить на компьютер новую версию Kaspersky Internet Security.

- Установка программы с установочного диска или дистрибутива (на стр. [16](#)).

Выполняется с помощью программы установки. Позволяет проверить наличие на веб-сайте Kaspersky Protection Center (см. раздел «О веб-сайте Kaspersky Protection Center» на стр. [16](#)) новой версии Kaspersky Internet Security, загрузить ее на компьютер и установить программу.

В ЭТОМ РАЗДЕЛЕ

Загрузка программы с последующей установкой с веб-сайта Kaspersky Protection Center..... [15](#)

Установка программы с установочного диска или дистрибутива [16](#)

ЗАГРУЗКА ПРОГРАММЫ С ПОСЛЕДУЮЩЕЙ УСТАНОВКОЙ С ВЕБ-САЙТА KASPERSKY PROTECTION CENTER

После того, как вы вошли на веб-сайт Kaspersky Protection Center (см. раздел «О веб-сайте Kaspersky Protection Center» на стр. [16](#)) с помощью Kaspersky Account (см. раздел «О Kaspersky Account» на стр. [15](#)) и скачали файл Kaspersky Internet Security.dmg, автоматически откроется окно с содержимым дистрибутива.

Если окно с содержимым дистрибутива автоматически не открылось, перейдите в папку на вашем компьютере, в которой хранится файл Kaspersky Internet Security.dmg и запустите его вручную.

➤ *Чтобы выполнить установку Kaspersky Internet Security,*


в окне с содержимым дистрибутива откройте установочный пакет **Установить Kaspersky Internet Security**.

Запустится программа установки Kaspersky Internet Security. Программа установки загрузит с веб-сайта Kaspersky Protection Center и установит на компьютер новую версию Kaspersky Internet Security (см. раздел «Установка программы с установочного диска или дистрибутива» на стр. [16](#)).

О KASPERSKY ACCOUNT

Kaspersky Account – это единая учетная запись для доступа ко всем сервисам «Лаборатории Касперского». Учетная запись Kaspersky Account используется для доступа на веб-сайт Kaspersky Protection Center (см. раздел «О веб-сайте Kaspersky Protection Center» на стр. [16](#)), а также к Личному кабинету на веб-сайте Службы технической поддержки. Если вы зарегистрированы в Личном кабинете, то значит у вас есть Kaspersky Account.

Для перехода к созданию Kaspersky Account или входа на веб-сайт Kaspersky Protection Center с помощью

Kaspersky Account откройте главное окно программы (на стр. [20](#)), нажмите на кнопку  и в открывшемся окне нажмите на кнопку **Kaspersky Account**.

Учетная запись Kaspersky Account представляет собой ваш адрес электронной почты и пароль, которые вы указали при создании учетной записи Kaspersky Account. Пароль должен содержать хотя бы восемь символов, одну цифру и одну прописную букву.

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

После активации учетной записи Kaspersky Account вы можете использовать ее для авторизации на веб-сайте Kaspersky Protection Center и в Личном кабинете. Если вы не активируете учетную запись Kaspersky Account по ссылке из письма в течение двух недель, она будет удалена.

Если у вас уже есть учетная запись Kaspersky Account, вы можете использовать ее для работы с Kaspersky Internet Security и доступа на веб-сайт Kaspersky Protection Center и к Личному кабинету.

О ВЕБ-САЙТЕ KASPERSKY PROTECTION CENTER

Веб-сайт Kaspersky Protection Center – это единый онлайн-ресурс для управления защитой всех ваших устройств и лицензированием программ «Лаборатории Касперского».

На веб-сайте Kaspersky Protection Center вы можете приобрести лицензию или продлить срок действия лицензии на использование Kaspersky Internet Security, загрузить новую версию программы на ваш компьютер, а также получить информацию об используемых программой антивирусных базах.

Для авторизации на веб-сайте Kaspersky Protection Center используется учетная запись Kaspersky Account (см. раздел «О Kaspersky Account» на стр. [15](#)).

УСТАНОВКА ПРОГРАММЫ С УСТАНОВОЧНОГО ДИСКА ИЛИ ДИСТРИБУТИВА

Окна программы установки **Лицензионное соглашение** и **Участие в Kaspersky Security Network** отображаются только для установки Kaspersky Internet Security на немецком и на русском языках. В остальных случаях с текстом Лицензионного соглашения и информацией об участии в Kaspersky Security Network вы можете ознакомиться, перейдя по соответствующим ссылкам в окне программы установки Kaspersky Internet Security.

➡ *Чтобы выполнить установку Kaspersky Internet Security с установочного диска или дистрибутива, выполните следующие действия:*

1. Откройте содержимое дистрибутива Kaspersky Internet Security:
 - если вы приобрели коробочную версию программы, вставьте установочный диск в дисковод;
 - если вы купили Kaspersky Internet Security в интернет-магазине и скачали дистрибутив программы в формате DMG на веб-сайте «Лаборатории Касперского», запустите dmg-файл.
2. В окне с содержимым дистрибутива откройте установочный пакет **Установить Kaspersky Internet Security**.

Запустится программа установки Kaspersky Internet Security. Программа установки начнет проверять наличие на веб-сайте Kaspersky Protection Center новой версии Kaspersky Internet Security.

3. Выберите действие по результатам проверки на наличие новой версии:
 - Если вы хотите пропустить проверку наличия новой версии Kaspersky Internet Security на веб-сайте Kaspersky Protection Center, нажмите на кнопку **Пропустить**, а затем на кнопку **Установить**.
Программа установки начнет установку на ваш компьютер версии Kaspersky Internet Security с установочного диска или дистрибутива.
 - Если программа установки обнаружит на веб-сайте Kaspersky Protection Center новую версию Kaspersky Internet Security, вы можете загрузить ее на компьютер и установить. Для этого нажмите на кнопку **Загрузить и установить**.
 - Если программа установки не обнаружит на веб-сайте Kaspersky Protection Center новую версию Kaspersky Internet Security, вы можете установить на компьютер версию Kaspersky Internet Security с установочного диска или дистрибутива. Для этого нажмите на кнопку **Установить**.

4. В окне **Лицензионное соглашение** ознакомьтесь с текстом Лицензионного соглашения об использовании Kaspersky Internet Security, которое заключается между вами и ЗАО «Лаборатория Касперского». После ознакомления с текстом Лицензионного соглашения выполните одно из следующих действий:

- Если вы согласны с условиями Лицензионного соглашения, нажмите на кнопку **Принять**.

Установка Kaspersky Internet Security будет продолжена.

- Если вы не согласны с условиями Лицензионного соглашения, нажмите на кнопку **Отмена**.

Установка программы будет отменена.

5. В окне **Участие в Kaspersky Security Network** прочтите информацию об участии в Kaspersky Security Network.

Участие в Kaspersky Security Network предусматривает отправку в ЗАО «Лаборатория Касперского» информации о новых угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о загружаемых подписанных программах, отправку уникального идентификатора, присвоенного вашему экземпляру Kaspersky Internet Security, и информации о системе. Гарантируется, что персональные данные не отправляются.

6. Если вы согласны со всеми пунктами положения об использовании Kaspersky Security Network, установите флажок **Я принимаю условия участия в Kaspersky Security Network**.

Если вы не согласны с условиями участия в Kaspersky Security Network, не устанавливайте флажок **Я принимаю условия участия в Kaspersky Security Network**.

В дальнейшем при использовании Kaspersky Internet Security вы можете в любой момент присоединиться к Kaspersky Security Network или отказаться от участия в Kaspersky Security Network.

7. Чтобы продолжить установку программы, нажмите на кнопку **Установить**.
8. Подтвердите установку Kaspersky Internet Security в окне запроса учетных данных администратора компьютера.
- Начнется установка Kaspersky Internet Security на ваш компьютер.
9. Нажмите на кнопку **Готово** для завершения работы программы установки.

По завершении установки Kaspersky Internet Security запускается автоматически. Перезагрузка компьютера не требуется.

ПОДГОТОВКА ПРОГРАММЫ К РАБОТЕ

После установки Kaspersky Internet Security рекомендуется выполнить следующие действия:

- Активировать Kaspersky Internet Security (см. раздел «Активация Kaspersky Internet Security» на стр. [31](#)). Активация программы позволит вам регулярно обновлять антивирусные базы и модули программы и обеспечит доступ к сервисам Службы технической поддержки.
- Оценить текущее состояние защиты компьютера (см. раздел «Оценка состояния защиты компьютера» на стр. [35](#)).
- Обновить Kaspersky Internet Security (см. раздел «Как обновить базы программы» на стр. [41](#)).
- Выполнить полную проверку компьютера на вирусы и другие программы, представляющие угрозу (см. раздел «Как выполнить полную проверку компьютера на вирусы» на стр. [39](#)).

УДАЛЕНИЕ ПРОГРАММЫ

В случае удаления Kaspersky Internet Security безопасность компьютера и ваших личных данных может оказаться под угрозой.

Рекомендуется перед удалением программы восстановить все объекты, расположенные в хранилище карантина. Все необработанные объекты удаляются из хранилища карантина без возможности восстановления.

➔ Чтобы удалить Kaspersky Internet Security, выполните следующие действия:

1. Откройте содержимое дистрибутива Kaspersky Internet Security:
 - если вы приобрели коробочную версию программы, вставьте установочный диск в дисковод;
 - если вы купили Kaspersky Internet Security в интернет-магазине и скачали дистрибутив программы в формате DMG на веб-сайте «Лаборатории Касперского», запустите dmg-файл.
2. В окне с содержимым дистрибутива откройте установочный пакет **Удалить Kaspersky Internet Security**.
Следуйте шагам программы удаления, чтобы удалить Kaspersky Internet Security.
3. В окне **Введение** нажмите на кнопку **Удалить**.
4. Подтвердите удаление программы в окне запроса учетных данных администратора компьютера.
Начнется удаление Kaspersky Internet Security с вашего компьютера.
5. В окне **Завершение** прочитайте информацию об окончании процесса удаления и нажмите на кнопку **Готово** для завершения работы программы удаления.

Перезагрузка компьютера после удаления Kaspersky Internet Security не требуется.

ИНТЕРФЕЙС ПРОГРАММЫ

Этот раздел содержит описание основных элементов графического интерфейса Kaspersky Internet Security: значка программы и контекстного меню значка программы, главного окна и окна настройки программы, окна Родительского контроля. Также раздел содержит информацию об окнах уведомлений и всплывающих сообщениях программы.

В ЭТОМ РАЗДЕЛЕ

Значок Kaspersky Internet Security	19
Главное окно программы	20
Окно настройки программы	21
Окно настройки Родительского контроля	22
Окна уведомлений и всплывающие сообщения	23
Новостной агент	24

ЗНАЧОК KASPERSKY INTERNET SECURITY

Сразу после установки Kaspersky Internet Security значок программы появляется в строке меню. Значок программы служит индикатором работы программы. Если значок программы активен, это означает, что защита компьютера от вредоносных программ в реальном времени включена. Неактивный значок программы свидетельствует о том, что защита выключена.

Значок Kaspersky Internet Security всегда располагается в строке меню. Если открыто какое-либо окно программы, значок Kaspersky Internet Security также отображается в панели быстрого запуска **Dock**.

Контекстное меню значка программы обеспечивает доступ к основным командам Kaspersky Internet Security:

- выключение защиты компьютера;
- возобновление защиты компьютера;
- переход к Центру защиты;
- запуск задачи обновления;
- запуск быстрой проверки компьютера на вирусы;
- переход к окну настройки Родительского контроля;
- переход к окну настройки программы.

➡ *Чтобы открыть контекстное меню значка Kaspersky Internet Security,*

нажмите на значок программы в строке меню.

ГЛАВНОЕ ОКНО ПРОГРАММЫ

➔ Чтобы открыть главное окно программы, выполните следующие действия:

1. Нажмите на значок Kaspersky Internet Security в строке меню.
2. В открывшемся контекстном меню значка программы выберите пункт **Kaspersky Internet Security**.

Задачи главного окна программы

В главном окне Kaspersky Internet Security вы можете просматривать информацию о состоянии защиты компьютера, работе Файлового Антивируса, Веб-Антивируса и выполнении задач поиска вирусов и задачи обновления.

Кроме того в главном окне программы вы можете выполнять следующие действия:

- запускать задачи поиска вирусов и задачи обновления;
- переходить к управлению ключами программы;
- открывать окно Центра защиты, окно настройки программы, окно отчетов;
- переходить к просмотру новостей о Kaspersky Internet Security и защите от компьютерных угроз в целом.

Элементы управления главного окна программы

Существует три возможных состояния защиты компьютера (см. раздел «Оценка состояния защиты компьютера» на стр. [35](#)).

О текущем состоянии защиты сигнализирует цвет индикатора состояния защиты компьютера:

- зеленый цвет означает, что защита вашего компьютера осуществляется на должном уровне;
- желтый и красный цвета сигнализируют о наличии проблем в настройке параметров или работе Kaspersky Internet Security.

Для получения подробной информации об этих проблемах и для их устранения вы можете воспользоваться Центром защиты (см. раздел «Использование Центра защиты» на стр. [37](#)). Окно Центра защиты открывается при нажатии на индикатор состояния защиты компьютера.

В левой части главного окна программы, в дополнение к индикатору состояния защиты компьютера, приведена текстовая информация о состоянии защиты компьютера, а также перечислены проблемы и угрозы безопасности, зафиксированные Центром защиты. Если на текущий момент запущены задачи поиска вирусов или задача обновления, информация о процессе их выполнения (в процентах) также выносится в левую часть главного окна программы.

С помощью кнопок главного окна программы вы можете выполнить следующие действия:



Запустить обновление Kaspersky Internet Security. По окончании обновления в окне отчетов представлена детальная информация о выполнении задачи обновления.



Перейти к задачам поиска вирусов: Быстрая проверка, Полная проверка и Поиск вирусов в указанной пользователем области. По завершении поиска вирусов в окне отчетов представлена детальная информация о выполнении задачи.



Перейти к окну, в котором представлена информация о лицензии (см. раздел «Просмотр информации о лицензии» на стр. [29](#)), и получить доступ к управлению ключами программы.

В верхней части главного окна программы расположена навигационная панель. С помощью кнопок навигационной панели вы можете выполнить следующие действия:



Открыть окно отчетов Kaspersky Internet Security, а также получить доступ к карантину.



Открыть окно настройки программы (на стр. [21](#)).





Открыть электронную справку Kaspersky Internet Security.



Открыть окно с информацией о способах получения технической поддержки (см. раздел «Обращение в Службу технической поддержки» на стр. [55](#)).



Открыть окно новостного агента со списком новостей (см. раздел «Новостной агент» на стр. [24](#)). Кнопка отображается после получения Kaspersky Internet Security новости.


В нижней части главного окна программы расположена кнопка . Нажмите на кнопку, чтобы развернуть панель, в которой приведена сводная статистика работы Файлового Антивируса, а также информация об используемых программой антивирусных базах. Чтобы свернуть панель, нажмите на кнопку  еще раз.

Также в нижней части главного окна программы расположены индикаторы работы Файлового Антивируса, Веб-Антивируса и Родительского контроля. Зеленый цвет индикатора означает, что компонент работает; красный цвет сигнализирует о том, что произошел сбой в работе компонента; серый цвет означает, что компонент выключен или не установлен.

С помощью кнопок, расположенных рядом с индикаторами работы Файлового Антивируса, Веб-Антивируса и Родительского контроля, вы можете перейти к настройке параметров этих компонентов.

ОКНО НАСТРОЙКИ ПРОГРАММЫ


Окно настройки параметров Kaspersky Internet Security можно открыть одним из следующих способов:


- нажав на кнопку  в главном окне программы (см. раздел «Главное окно программы» на стр. [20](#));
- выбрав пункт **Настройка** в контекстном меню значка Kaspersky Internet Security (см. раздел «Значок Kaspersky Internet Security» на стр. [19](#)).

Для быстрого доступа к параметрам программы вы можете использовать следующие закладки, расположенные в верхней части окна настройки:

- **Защита.** На закладке вы можете настроить параметры Файлового Антивируса и Веб-Антивируса.
- **Поиск вирусов.** На закладке вы можете настроить параметры задач поиска вирусов.
- **KSN.** На закладке вы можете присоединиться к Kaspersky Security Network или отказаться от участия в Kaspersky Security Network.
- **Угрозы.** На закладке вы можете выбрать категории обнаруживаемых объектов и сформировать доверенную зону.
- **Обновление.** На закладке вы можете настроить параметры обновления программы
- **Отчеты.** На закладке вы можете настроить параметры отчетов Kaspersky Internet Security и карантина.
- **Вид.** На закладке вы можете настроить параметры отображения окон уведомлений Kaspersky Internet Security.

Вы можете запретить пользователям, не имеющим прав администратора компьютера, изменять параметры

работы Kaspersky Internet Security с помощью кнопки . Кнопка расположена в нижней части окна настройки. Чтобы снять ограничения на изменение параметров, потребуется ввести учетные данные администратора компьютера.

Кнопка  обеспечивает доступ к справочной системе Kaspersky Internet Security с описанием параметров текущего окна программы. Также вы можете открыть справку для текущего окна программы, выбрав в меню Справка пункт **Открыть справку для этого окна**.

Окно НАСТРОЙКИ РОДИТЕЛЬСКОГО КОНТРОЛЯ

Окно настройки Родительского контроля можно открыть одним из следующих способов:

- выбрать пункт **Родительский контроль** в контекстном меню значка Kaspersky Internet Security (см. раздел «Значок Kaspersky Internet Security» на стр. [19](#));
- нажать на кнопку, расположенную рядом с индикатором работы Родительского контроля, в нижней части главного окна программы (см. раздел «Главное окно программы» на стр. [20](#)).

В левой части окна настройки Родительского контроля расположен список учетных записей пользователей компьютера. Рядом с именем учетной записи отображается индикатор работы Родительского контроля для этой учетной записи. Зеленый цвет индикатора означает, что Родительский контроль включен; красный цвет сигнализирует о том, что Родительский контроль выключен. По умолчанию Родительский контроль выключен для всех учетных записей пользователей компьютера. Вы можете его включить.

Если Родительский контроль для учетной записи пользователя включен, то в правой части окна настройки Родительского контроля на закладке **Настройка** вы можете выбрать, какие действия этого пользователя на компьютере и в интернете нужно контролировать.

Kaspersky Internet Security осуществляет контроль следующих действий пользователя по категориям:

- **Веб-контроль** – контроль посещаемых веб-сайтов и загружаемых файлов.
- **Контроль времени** – контроль времени доступа в интернет.
- **Персональные данные** – контроль использования персональных данных.
- **Социальные сети** – контроль использования социальных сетей.

По умолчанию контроль действий пользователя выключен для всех категорий. Вы можете его включить отдельно для каждой категории действий пользователя и перейти к более детальной настройке выбранной категории в правой части окна настройки Родительского контроля.

Также для каждой учетной записи пользователя, для которой включен Родительский контроль, в правой части окна настройки Родительского контроля на закладке **Отчеты** вы можете просмотреть отчеты о действиях и активности пользователя, отдельно для каждой категории.

Пользователи, не имеющие прав администратора компьютера, не могут осуществлять настройку Родительского контроля. Для настройки и просмотра отчетов Родительского контроля вам потребуется нажать на кнопку



и ввести учетные данные администратора компьютера.

ОКНА УВЕДОМЛЕНИЙ И ВСПЛЫВАЮЩИЕ СООБЩЕНИЯ

Во время работы Kaspersky Internet Security возникают события разных уровней важности.

Программа информирует вас о возникновении событий с помощью *окон уведомлений* и *всплывающих сообщений*, которые могут дополняться звуковым оповещением.

Kaspersky Internet Security поддерживает технологию Growl для вывода окон уведомлений. Если технология Growl подключена, всплывающие экранные сообщения выводятся с ее использованием.

В ЭТОМ РАЗДЕЛЕ

Об окнах уведомлений.....	23
О типах событий.....	23
О всплывающих сообщениях	23
Выключение доставки уведомлений.....	24

ОБ ОКНАХ УВЕДОМЛЕНИЙ

Kaspersky Internet Security выводит на экран окно уведомления в случае, когда при возникновении события вам нужно выбрать вариант действия. Например, когда программа обнаруживает вредоносный объект, она предлагает вам удалить объект или лечить его. Окно уведомления исчезнет с экрана только после того, как вы выберете одно из предложенных действий.

О ТИПАХ СОБЫТИЙ

События в работе Kaspersky Internet Security по уровню важности делятся на три типа:

- **Критические** – события, представляющие серьезную угрозу безопасности компьютера (обнаружение вредоносных объектов, уязвимостей, проблем в работе Kaspersky Internet Security). При возникновении критических событий требуются немедленные действия пользователя. Рекомендуется не отключать уведомления о критических событиях.
- **Важные** – события, которые не требуют немедленных действий пользователя, но в дальнейшем могут представлять угрозу для безопасности компьютера.
- **Информационные события** – события справочного характера.

О ВСПЛЫВАЮЩИХ СООБЩЕНИЯХ


Kaspersky Internet Security выводит на экран *всплывающие сообщения*, чтобы проинформировать вас о событиях, не требующих обязательного выбора действия. Всплывающие сообщения появляются под значком программы в строке меню и автоматически исчезают с экрана вскоре после появления.

ВЫКЛЮЧЕНИЕ ДОСТАВКИ УВЕДОМЛЕНИЙ


По умолчанию Kaspersky Internet Security уведомляет (см. раздел «Окна уведомлений и всплывающие сообщения» на стр. [23](#)) вас о всех событиях, связанных с работой программы. Вы можете отключить доставку уведомлений или выбрать типы событий, уведомления о которых вы не хотите получать, а также выключить звуковое оповещение.

Вне зависимости от того, включена или выключена доставка уведомлений, информация о событиях, возникающих в ходе работы Kaspersky Internet Security, записывается в отчет о работе программы.


➤ *Чтобы выключить доставку уведомлений, выполните следующие действия:*

1. Нажмите на кнопку  в главном окне программы (см. раздел «Главное окно программы» на стр. [20](#)).
Откроется окно настройки программы.
2. На закладке **Вид** окна настройки программы в блоке **Уведомления** снимите флажок **Уведомлять о событиях**, чтобы не получать уведомления в виде окон уведомлений.

➤ *Чтобы выбрать типы событий, уведомления о которых вы не хотите получать, выполните следующие действия:*

1. Нажмите на кнопку  в главном окне программы (см. раздел «Главное окно программы» на стр. [20](#)).
Откроется окно настройки программы.
2. На закладке **Вид** окна настройки программы в блоке **Уведомления** снимите флажки рядом с названиями тех типов событий (см. раздел «О типах событий» на стр. [23](#)), уведомления о которых вы не хотите получать.


➤ *Чтобы выключить звуковое оповещение при появлении окон уведомлений и всплывающих сообщений, выполните следующие действия:*

1. Нажмите на кнопку  в главном окне программы (см. раздел «Главное окно программы» на стр. [20](#)).
Откроется окно настройки программы.
2. На закладке **Вид** окна настройки программы в блоке **Уведомления** снимите флажок **Включить звуковое сопровождение уведомлений**.

НОВОСТНОЙ АГЕНТ

С помощью новостного агента «Лаборатория Касперского» информирует вас о новостях, касающихся Kaspersky Internet Security и защиты от компьютерных угроз в целом.



Программа уведомляет вас о появлении новостей с помощью значка  в верхней части главного окна программы (см. раздел «Главное окно программы» на стр. [20](#)). При нажатии на значок отображается окно **Новости**.

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	25
О лицензии.....	25
О подписке	26
О коде активации.....	27
О предоставлении данных.....	27
Просмотр информации о лицензии.....	29
Приобретение лицензии	29
Продление срока действия лицензии	30
Продление подписки	30
Обновление статуса подписки	30
Активация Kaspersky Internet Security.....	31

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 ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения. С лицензией связан уникальный код активации вашего экземпляра Kaspersky Internet Security.

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](#)).

Чтобы работать с программой, вы должны приобрести лицензию на использование программы.

Лицензия имеет ограниченный срок действия. По истечении срока действия лицензии программа продолжает работу, но в режиме ограниченной функциональности (например, недоступно обновление и использование сервиса Kaspersky Security Network). Вы по-прежнему можете использовать все компоненты программы и выполнять проверку на вирусы и другие программы, представляющие угрозу, но только на основе антивирусных баз, установленных до даты окончания срока действия лицензии. Для продолжения использования Kaspersky Internet Security в режиме полной функциональности требуется продлить срок действия лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от всех угроз компьютерной безопасности.

Перед приобретением лицензии вы можете ознакомиться с пробной версией Kaspersky Internet Security без выплаты вознаграждения. Пробная версия Kaspersky Internet Security выполняет свои функции в течение короткого ознакомительного периода. После окончания ознакомительного периода Kaspersky Internet Security прекращает выполнять все свои функции. Для продолжения использования программы требуется приобрести лицензию.

О ПОДПИСКЕ

Подписка на Kaspersky Internet Security – это заказ на использование программы с выбранными параметрами (дата окончания, количество защищаемых устройств). Подписку на Kaspersky Internet Security можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Вы можете приостанавливать или возобновлять подписку, продлевать ее в автоматическом режиме, а также отказываться от нее. Подпиской можно управлять через ваш персональный кабинет на веб-сайте поставщика услуги.

Поставщики услуг могут предоставлять два типа подписки на использование Kaspersky Internet Security: подписку на обновление и подписку на обновление и защиту.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Internet Security после окончания ограниченной подписки необходимо самостоятельно продлить ее. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее окончании вам будет предоставлен льготный период для продления подписки, в течение которого функциональность программы будет сохранена.

Если подписка не продлена, по истечении льготного периода Kaspersky Internet Security прекращает обновление баз программы (для подписки на обновление), а также прекращает осуществлять защиту компьютера и запускать задачи проверки (для подписки на обновление и защиту).

Чтобы использовать Kaspersky Internet Security по подписке, нужно применить код активации, предоставленный поставщиком услуг. В некоторых случаях код активации может загружаться и применяться автоматически. При использовании программы по подписке вы не можете применить другой код активации для продления срока действия лицензии. Это будет возможно только после окончания подписки.

Если на момент регистрации подписки Kaspersky Internet Security уже используется по действующей лицензии, то после регистрации подписки Kaspersky Internet Security будет использоваться по подписке. Код активации, с помощью которого до этого была активирована программа, можно применить на другом компьютере.

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

В зависимости от поставщика услуг, набор возможных действий при управлении подпиской может различаться. Кроме того, может не предоставляться льготный период, в течение которого доступно продление подписки.

О КОДЕ АКТИВАЦИИ

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

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

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».

О ПРЕДОСТАВЛЕНИИ ДАННЫХ

Для повышения уровня оперативной защиты, принимая условия Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять «Лаборатории Касперского» информацию об установке, используемой версии и настройках ПО, а также информацию об активации.

При участии в Kaspersky Security Network в «Лабораторию Касперского» автоматически передается следующая информация, полученная в результате работы Kaspersky Internet Security на компьютере:

- Информация об установленном на компьютере аппаратном и программном обеспечении, в том числе версия операционной системы и установленные пакеты обновлений, загруженные объекты.
- Информация о состоянии антивирусной защиты компьютера, а также данные обо всех потенциально вредоносных объектах и действиях (в том числе название детектируемого объекта, хеш-сумма (MD5), дата и время обнаружения, URL-адрес, по которому он был загружен, названия и размер зараженных файлов и пути к ним, IP-адрес атакующего компьютера и номер порта компьютера пользователя, на который была направлена сетевая атака, перечень активностей вредоносной программы, потенциально вредоносные URL-адреса) и решениях продукта и пользователя по ним.
- Информация о загружаемых пользователем программах (URL-адрес, атрибуты, размер файла, информация о процессе, загрузившем файл).
- Информация о запускаемых программах и их модулях (размер, атрибуты, дата создания, информация заголовка PE, регион, имя, местоположение, упаковки).
- Информация об ошибках и использовании пользовательского интерфейса установленного продукта «Лаборатории Касперского».

В случае возникновения ошибки в процессе работы Kaspersky Internet Security в «Лабораторию Касперского» пользователем может быть отправлен файл, содержащий следующую информацию:

- название и идентификатор процесса;
- путь к исполняемому модулю;
- версия программы;
- битность процесса (32- или 64-бит);
- название и идентификатор родительского процесса;
- время и дата падения программы;
- версия операционной системы;
- версия отчета;
- тип ошибки, приведшей к падению программы;
- информация об ошибке;
- номер потока, в котором возникла ошибка;
- стеки выполнения для каждого потока во время падения программы (номер фрейма, название модуля, адрес в коде, название функции по соответствующему адресу);
- значения регистров потока, в котором возникла ошибка;
- список загруженных модулей с указанием адреса, по которому загружен модуль, названия модуля, его версии, UUID и пути к нему;

Дополнительно для операционной системы Mountain Lion указывается следующая информация:


- ID пользователя (UID);
- статистика вызова определенных системных вызовов взаимодействия других процессов с данным процессом;
- распределение памяти (статистика количества памяти, выделенного под те или иные области).

Также для дополнительной проверки в «Лабораторию Касперского» могут отправляться файлы, в отношении которых существует риск использования их злоумышленником с целью нанесения вреда компьютеру пользователя, или их части.

Полученная информация защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями. «Лаборатория Касперского» использует полученную информацию только в виде общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных данных и иной конфиденциальной информации. Исходная полученная информация хранится в зашифрованном виде и уничтожается по мере накопления (два раза в год). Данные общей статистики хранятся бессрочно.

ПРОСМОТР ИНФОРМАЦИИ О ЛИЦЕНЗИИ

➔ Чтобы просмотреть информацию о лицензии,

откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .

Откроется окно **Лицензия**.

В открывшемся окне **Лицензия** содержится следующая информация о лицензировании программы:

- ключ;
- статус ключа или подписки;
- ограничение на количество компьютеров, на которых вы можете использовать программу;
- дата и время окончания срока действия лицензии;
- остаток дней до окончания срока действия лицензии.

Если лицензия отсутствует, то Kaspersky Internet Security сообщит вам об этом. Если программа не активирована, вы можете начать процедуру активации (см. раздел «Активация Kaspersky Internet Security» на стр. [31](#)). Если вы используете пробную версию программы, вы можете приобрести лицензию (см. раздел «Приобретение лицензии» на стр. [29](#)).


По лицензии вы можете добавить два ключа: активный и резервный. Активный ключ используется с момента активации программы. Резервный ключ автоматически получает статус активного сразу по окончании срока действия лицензии, связанной с активным ключом. Если резервный ключ не был добавлен, а срок действия лицензии, связанной с активным ключом, истекает, вы можете продлить срок ее действия (см. раздел «Продление срока действия лицензии» на стр. [30](#)).

Если ваша подписка на Kaspersky Internet Security истекла и истек льготный период, в течение которого доступно продление подписки, вы можете продлить подписку вручную (см. раздел «Продление подписки» на стр. [30](#)). Также при использовании программы по подписке вы можете выполнить обновление статуса подписки (на стр. [30](#)).

ПРИБРЕТЕНИЕ ЛИЦЕНЗИИ

Если лицензия на использование Kaspersky Internet Security отсутствует или вы используете пробную версию программы, вы можете приобрести лицензию.

➔ Чтобы приобрести лицензию, выполните следующие действия:


1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Приобрести**.

Откроется веб-страница с информацией об условиях приобретения лицензии через интернет-магазин «Лаборатории Касперского» либо у партнеров компании. По факту оплаты при приобретении лицензии через интернет-магазин вам будет отправлен код активации Kaspersky Internet Security (см. раздел «О коде активации» на стр. [27](#)) на электронный адрес, указанный в форме заказа.

ПРОДЛЕНИЕ СРОКА ДЕЙСТВИЯ ЛИЦЕНЗИИ

Необходимость продления срока действия лицензии на использование программы возникает по истечении срока действия имеющейся лицензии, связанной с активным ключом, если резервный ключ не был добавлен. В случае если срок действия лицензии не продлен, Kaspersky Internet Security продолжает выполнять все свои функции, однако обновление антивирусных баз не производится.

➤ *Чтобы продлить срок действия лицензии, выполните следующие действия:*

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Продлить**.

Откроется веб-страница с информацией об условиях продления срока действия лицензии через интернет-магазин «Лаборатории Касперского» либо у партнеров компании. По факту оплаты при продлении срока действия лицензии через интернет-магазин вам будет отправлен код активации Kaspersky Internet Security (см. раздел «О коде активации» на стр. [27](#)) на электронный адрес, указанный в форме заказа.

ПРОДЛЕНИЕ ПОДПИСКИ


При использовании программы по подписке Kaspersky Internet Security автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки.

Если вы используете программу по неограниченной подписке, Kaspersky Internet Security самостоятельно в фоновом режиме проверяет наличие обновленного ключа на сервере активации и в случае его наличия, добавляет его в режиме замены предыдущего ключа. Таким образом неограниченная подписка на Kaspersky Internet Security продлевается без вашего участия.

Если подписка истекла и истек льготный период, в течение которого доступно продление подписки, Kaspersky Internet Security уведомляет вас об этом и прекращает попытки автоматического продления подписки. Kaspersky Internet Security прекращает обновление баз программы (для подписки на обновление), а также прекращает осуществлять защиту компьютера и запускать задачи проверки (для подписки на обновление и защиту).

Вы можете продлить подписку вручную, связавшись с поставщиком услуг, у которого вы приобрели Kaspersky Internet Security.

➤ *Чтобы продлить подписку, выполните следующие действия:*

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Посетить веб-сайт поставщика услуг**.


На открывшейся веб-странице представлена информация об условиях продления подписки.

ОБНОВЛЕНИЕ СТАТУСА ПОДПИСКИ

При использовании программы по подписке вы можете обратиться к серверу активации для получения информации об используемом ключе.

Необходимость обновления статуса подписки возникает, если по каким-либо причинам подписка не была продлена вовремя (например, компьютер был выключен весь период, когда было доступно продление подписки). До момента продления подписки Kaspersky Internet Security прекращает обновление антивирусных баз (для подписки на обновление), а также прекращает осуществлять защиту компьютера и запускать задачи проверки (для подписки на обновление и защиту).

➤ Чтобы обновить статус подписки, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Обновить статус подписки**.

АКТИВАЦИЯ KASPERSKY INTERNET SECURITY

Перед активацией Kaspersky Internet Security убедитесь в том, что параметры системной даты компьютера соответствуют фактической дате и времени.

Процедура активации программы заключается в добавлении активного ключа, на основании которого Kaspersky Internet Security проверяет наличие прав на использование программы и определяет срок ее использования.

Если программа не активирована, вам доступны все функции Kaspersky Internet Security, за исключением получения обновлений. Обновление антивирусных баз можно выполнить только один раз после установки программы.

В ЭТОМ РАЗДЕЛЕ

Активация пробной версии программы	31
Активация программы с помощью кода активации.....	32


АКТИВАЦИЯ ПРОБНОЙ ВЕРСИИ ПРОГРАММЫ

Активация пробной версии программы возможна только в том случае, если пробная версия Kaspersky Internet Security ранее не устанавливалась на этот компьютер.

Рекомендуется активировать пробную версию программы в случае, если вы хотите ознакомиться с программой перед принятием решения о приобретении лицензии. Для активации пробной версии программы на короткий ознакомительный период вам будет предоставлен бесплатный ключ.

При активации пробной версии программы требуется подключение к интернету. Если на текущий момент соединение с интернетом отсутствует, вы можете провести активацию пробной версии программы позже.

➤ Чтобы активировать пробную версию программы, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Пробная версия**.
3. В окне **Активация пробной версии программы** нажмите на кнопку **Активировать пробную версию**.

Kaspersky Internet Security осуществит соединение с серверами «Лаборатории Касперского» и отправит данные для проверки. В случае успешной проверки программа получит и добавит на короткий ознакомительный период бесплатный ключ.

После успешной активации пробной версии программы откроется окно **Лицензия**, в котором вы можете просмотреть следующую информацию:

- статус ключа;
- ограничение на количество компьютеров, на которых вы можете использовать программу;
- дату и время окончания срока действия лицензии;
- остаток дней до окончания срока действия лицензии.

4. Нажмите на кнопку **Готово**, чтобы вернуться в главное окно программы (на стр. [20](#)).


По истечении короткого ознакомительного периода использования пробной версии Kaspersky Internet Security, на экране появится соответствующее уведомление. Для продолжения использования программы вы можете приобрести лицензию (см. раздел «Приобретение лицензии» на стр. [29](#)).

АКТИВАЦИЯ ПРОГРАММЫ С ПОМОЩЬЮ КОДА АКТИВАЦИИ

Рекомендуется использовать этот вариант активации, если вы приобрели лицензию на использование программы, зарегистрировали подписку на обновление или подписку на обновление и защиту и вам был предоставлен код активации. На основании кода активации вы получите ключ, обеспечивающий доступ к функциональности Kaspersky Internet Security на срок действия лицензии.

При выборе активации программы с помощью кода активации требуется подключение к интернету. Если на текущий момент соединение с интернетом отсутствует, вы можете провести активацию программы позже.

➔ Чтобы активировать программу с помощью кода активации, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Активировать**.
3. В окне **Активация программы** введите код активации, полученный при покупке Kaspersky Internet Security.

Код активации представляет собой последовательность цифр и букв, разделенных дефисами на четыре блока по пять символов, без пробелов, например, 11AA1-11AAA-1AA11-1A111. Код активации следует вводить латинскими символами.

Kaspersky Internet Security осуществит соединение с серверами «Лаборатории Касперского» и отправит код активации для проверки. В случае успешной проверки кода активации программа получит и добавит ключ.

В зависимости от предоставленного кода активации Kaspersky Internet Security может потребовать заполнения пользователем обязательной или необязательной регистрационной формы или регистрации в Личном кабинете (см. раздел «Получение технической поддержки через Личный кабинет» на стр. [56](#)).

Если код активации не прошел проверку, на экране появится соответствующее уведомление. В этом случае обратитесь за информацией в компанию, где вы приобрели Kaspersky Internet Security.

После успешной активации программы с помощью кода активации откроется окно **Лицензия**, в котором вы можете просмотреть следующую информацию:

- ключ;
- статус ключа или подписки;
- ограничение на количество компьютеров, на которых вы можете использовать программу;
- дата и время окончания срока действия лицензии;
- остаток дней до окончания срока действия лицензии.

4. Нажмите на кнопку **Готово**, чтобы вернуться в главное окно программы (на стр. [20](#)).

ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ

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

Сразу же после установки программа запускается автоматически, и значок Kaspersky Internet Security (на стр. [19](#)) появляется в строке меню.

◆ *Чтобы завершить работу Kaspersky Internet Security,*

нажмите на значок Kaspersky Internet Security (на стр. [19](#)) в строке меню и в открывшемся контекстном меню выберите пункт **Выход**.

Работа программы остановится, и процесс будет удален из оперативной памяти компьютера.

После завершения работы с Kaspersky Internet Security компьютер продолжит работать в незащищенном режиме и может быть подвергнут риску заражения, а ваши персональные данные окажутся под угрозой.

СОСТОЯНИЕ ЗАЩИТЫ КОМПЬЮТЕРА

Этот раздел содержит информацию о том, как определить наличие проблем и угроз безопасности компьютера и настроить уровень его защиты. Из этого раздела вы также узнаете о включении и отключении защиты во время работы программы.

Состояние защиты вашего компьютера отражает наличие или отсутствие на текущий момент угроз, влияющих на общий уровень безопасности операционной системы. К угрозам в этом случае относятся не только обнаруженные вредоносные программы, но и использование устаревших антивирусных баз, отключение Файлового Антивируса или Веб-Антивируса.

Центр защиты (см. раздел «Использование Центра защиты» на стр. [37](#)) поможет последовательно просмотреть имеющиеся угрозы и перейти к их устранению.

В ЭТОМ РАЗДЕЛЕ

Оценка состояния защиты компьютера	35
Выключение защиты компьютера	36
Возобновление защиты компьютера	37
Использование Центра защиты	37

ОЦЕНКА СОСТОЯНИЯ ЗАЩИТЫ КОМПЬЮТЕРА

О появлении проблем в защите компьютера сигнализирует индикатор состояния защиты компьютера, расположенный в правой части главного окна программы (см. раздел «Главное окно программы» на стр. [20](#)). В зависимости от состояния защиты компьютера цвет индикатора изменяется. При наличии угроз компьютерной безопасности индикатор дополняется сообщением об угрозах.

Индикатор может принимать одно из следующих значений:

- **Зеленый.** Защита вашего компьютера обеспечивается на должном уровне.

Зеленый цвет индикатора означает, что антивирусные базы программы актуальны, а все компоненты программы работают в соответствии с параметрами, рекомендованными специалистами «Лаборатории Касперского». Вредоносные объекты не обнаружены либо обезврежены. Родительский контроль работает в нормальном режиме.

- **Желтый.** Уровень защиты вашего компьютера снижен.

Желтый цвет индикатора свидетельствует о наличии проблем в работе Kaspersky Internet Security. Например, есть незначительные отклонения от рекомендуемого режима работы, антивирусные базы программы не обновлялись в течение нескольких дней.

- **Красный.** Ваш компьютер подвергается угрозе заражения.

Красный цвет индикатора сигнализирует о наличии серьезных проблем, которые могут привести к заражению компьютера и потере данных. Например, антивирусные базы программы сильно устарели, программа не активирована или обнаружены вредоносные объекты.

Проблемы и угрозы компьютерной безопасности рекомендуется немедленно устранять. Нажав на индикатор состояния защиты компьютера в главном окне программы, можно открыть окно Центр защиты (см. раздел «Использование Центра защиты» на стр. [37](#)), в котором приведена подробная информация о состоянии защиты компьютера и предложены варианты действий для устранения проблем и угроз.

ВЫКЛЮЧЕНИЕ ЗАЩИТЫ КОМПЬЮТЕРА

По умолчанию Kaspersky Internet Security запускается при старте операционной системы и защищает ваш компьютер в течение всего сеанса работы. Все компоненты защиты (Файловый Антивирус, Веб-Антивирус) включены и работают.

Вы можете полностью или частично выключить защиту, обеспечиваемую Kaspersky Internet Security.

Специалисты «Лаборатории Касперского» настоятельно рекомендуют не отключать защиту, обеспечиваемую Файловым Антивирусом и Веб-Антивирусом в режиме реального времени, поскольку это может привести к заражению вашего компьютера и потере данных.

Об отключении защиты компьютера свидетельствуют следующие признаки:

- неактивный значок программы (см. раздел «Значок Kaspersky Internet Security» на стр. [19](#)) в строке меню;
- красный цвет индикатора состояния защиты компьютера в правой части главного окна программы.

Защита компьютера рассматривается именно в контексте работы Файлового Антивируса и Веб-Антивируса. Отключение или приостановка работы этих компонентов защиты не оказывает влияния на выполнение задач поиска вирусов и задачи обновления.


Полностью выключить защиту компьютера можно несколькими способами. Выключить компоненты защиты можно на закладке **Защита** окна настройки программы.

➔ Чтобы выключить защиту компьютера, воспользуйтесь одним из следующих способов:

- Нажмите на значок Kaspersky Internet Security (на стр. [19](#)) в строке меню и в открывшемся контекстном меню выберите пункт **Выключить защиту**.
- Откройте окно настройки программы (на стр. [21](#)), выберите закладку **Защита** и в блоке **Основные** снимите флажок **Включить защиту**.

Если вы выключили защиту компьютера, то после перезапуска Kaspersky Internet Security она не включится автоматически. Требуется включить защиту компьютера вручную (см. раздел «Возобновление защиты компьютера» на стр. [37](#)).

➔ Чтобы выключить компонент защиты, выполните следующие действия:

1. Нажмите на кнопку  в главном окне программы (см. раздел «Главное окно программы» на стр. [20](#)).
Откроется окно настройки программы.
2. На закладке **Защита** окна настройки программы в блоке **<наименование компонента>** снимите флажок **Включить <наименование компонента>**.

Если вы выключили компонент защиты, то после перезапуска Kaspersky Internet Security он не включится автоматически. Требуется включить компонент защиты вручную (см. раздел «Возобновление защиты компьютера» на стр. [37](#)).


ВОЗОБНОВЛЕНИЕ ЗАЩИТЫ КОМПЬЮТЕРА

Если защита компьютера или компонент защиты (Файловый Антивирус или Веб-Антивирус) были выключены, то возобновить защиту компьютера или работу компонентов защиты можно только вручную по требованию пользователя. Автоматического включения защиты компьютера или компонентов защиты после перезагрузки операционной системы или Kaspersky Internet Security не происходит.

➤ Чтобы включить защиту компьютера, воспользуйтесь одним из следующих способов:

- Нажмите на значок Kaspersky Internet Security (на стр. [19](#)) в строке меню и в открывшемся контекстном меню выберите пункт **Включить защиту**.
- Откройте окно настройки программы (на стр. [21](#)), выберите закладку **Защита** и в блоке **Основные** установите флажок **Включить защиту**.

➤ Чтобы включить компонент защиты, выполните следующие действия:

1. Нажмите на  в главном окне программы (см. раздел «Главное окно программы» на стр. [20](#)).

Откроется окно настройки программы.

2. На закладке **Защита** окна настройки программы в блоке **<наименование компонента>** установите флажок **Включить <наименование компонента>**.

Также чтобы включить защиту компьютера или компоненты защиты вы можете воспользоваться Центром защиты (см. раздел «Использование Центра защиты» на стр. [37](#)). Выключение защиты компьютера или выключение компонентов защиты значительно повышает риск заражения компьютера, поэтому информация о выключении защиты сохраняется в Центре защиты.

ИСПОЛЬЗОВАНИЕ ЦЕНТРА ЗАЩИТЫ

Центр защиты – это сервис, который позволяет анализировать и устранять имеющиеся проблемы и угрозы компьютерной безопасности.

➤ Чтобы открыть Центр защиты,

нажмите на индикатор состояния защиты компьютера в главном окне программы (см. раздел «Главное окно программы» на стр. [20](#)).

В окне Центра защиты вы можете ознакомиться со списком существующих проблем и угроз компьютерной безопасности. Проблемы и угрозы сгруппированы по категориям, к которым они относятся. Для каждой проблемы или угрозы приведены действия, которые вы можете предпринять, чтобы решить проблему или устранить угрозу. Вы можете решить проблему или устранить угрозу немедленно или отложить решение проблемы или устранение угрозы.

➤ Чтобы устранить проблему или угрозу немедленно,

нажмите на кнопку с названием рекомендуемого действия для устранения проблемы или угрозы.

Например, если на компьютере обнаружены зараженные объекты, нужно нажать на кнопку **Лечить**. Если используемые программой антивирусные базы устарели, нужно нажать на кнопку **Обновить**. Программа выполнит выбранное действие.

➤ Чтобы отложить устранение проблемы или угрозы,

нажмите на кнопку **Скрыть**.

Сообщение о проблеме или угрозе будет скрыто в списке. Вы сможете вернуться к устранению этой проблемы или угрозы позже.

Вы не можете отложить устранение серьезных угроз компьютерной безопасности. К серьезным угрозам относятся, например, необработанные вредоносные объекты, сбои в работе компонентов защиты, повреждения баз Kaspersky Internet Security.

Если вы завершите работу с Центром защиты без устранения серьезных угроз, цвет индикатора состояния защиты компьютера в главном окне программы будет по-прежнему сигнализировать об их наличии.

Также в окне Центра защиты вы можете просмотреть информацию о задаче обновления или задачах поиска вирусов, выполняющихся в текущий момент, и при необходимости остановить или перезапустить задачи.

РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ

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

В ЭТОМ РАЗДЕЛЕ

Как выполнить полную проверку компьютера на вирусы	39
Как выполнить быструю проверку компьютера	40
Как проверить на вирусы файл, папку или диск.....	40
Как приобрести лицензию	40
Как продлить срок действия лицензии.....	41
Как обновить базы программы	41
Как защитить от перехвата данные, вводимые с клавиатуры	41
Как ограничить время работы пользователя в интернете	42
Как ограничить посещение веб-сайтов и загрузку файлов из интернета.....	43
Как ограничить контакты и переписку пользователя в социальных сетях	43
Как запретить пересылку персональных данных	44
Что делать, если программа заблокировала доступ к файлу.....	44
Как восстановить удаленный или вылеченный программой объект	45
Как просмотреть отчет о работе программы.....	46
Что делать при появлении окон уведомлений и всплывающих сообщений	46

КАК ВЫПОЛНИТЬ ПОЛНУЮ ПРОВЕРКУ КОМПЬЮТЕРА НА ВИРУСЫ

В Kaspersky Internet Security входит созданная по умолчанию задача полной проверки компьютера. Выполняя эту задачу, программа проверяет все жесткие диски компьютера на наличие вирусов и других программ, представляющих угрозу.

► Чтобы запустить задачу полной проверки компьютера, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .


2. В открывшемся меню выберите задачу  **Полная проверка.**


С результатами выполнения задачи можно ознакомиться в окне отчетов.

КАК ВЫПОЛНИТЬ БЫСТРУЮ ПРОВЕРКУ КОМПЬЮТЕРА

В Kaspersky Internet Security входит созданная по умолчанию задача быстрой проверки компьютера. Выполняя эту задачу, программа проверяет на вирусы и другие программы, представляющие угрозу, критические области компьютера: папки, содержащие файлы операционной системы и системные библиотеки, поражение которых вредоносными программами может привести к повреждению операционной системы вашего компьютера.

► Чтобы запустить задачу быстрой проверки компьютера, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .


2. В открывшемся меню выберите задачу  **Быстрая проверка.**

С результатами выполнения задачи можно ознакомиться в окне отчетов.

КАК ПРОВЕРИТЬ НА ВИРУСЫ ФАЙЛ, ПАПКУ ИЛИ ДИСК

Если вам требуется проверить на вирусы и другие программы, представляющие угрозу, отдельный объект (один из жестких дисков, отдельную папку, файл или съемное устройство), нужно воспользоваться встроенной задачей Поиск вирусов.

► Чтобы проверить на вирусы и другие программы, представляющие угрозу, отдельный объект, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .

2. В открывшемся меню выберите задачу  **Поиск вирусов.**

Откроется окно выбора объектов проверки.

3. Сформируйте список объектов проверки.


Задача поиска вирусов запустится автоматически.

С результатами выполнения задачи можно ознакомиться в окне отчетов.

КАК ПРИОБРЕСТИ ЛИЦЕНЗИЮ

Если вы установили Kaspersky Internet Security, не имея лицензии, вы можете приобрести лицензию уже после установки программы. При приобретении лицензии вы получаете код активации, с помощью которого нужно активировать программу (см. раздел «Активация Kaspersky Internet Security» на стр. [31](#)).

► Чтобы приобрести лицензию, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .


2. В открывшемся окне нажмите на кнопку **Приобрести.**

Откроется веб-страница интернет-магазина «Лаборатории Касперского», где вы можете приобрести лицензию.

КАК ПРОДЛИТЬ СРОК ДЕЙСТВИЯ ЛИЦЕНЗИИ

Если срок действия лицензии, по которой активирован Kaspersky Internet Security, подходит к концу, вы можете его продлить. При продлении срока действия лицензии вы получаете код активации, с помощью которого нужно активировать программу (см. раздел «Активация Kaspersky Internet Security» на стр. [31](#)).

► Чтобы продлить срок действия лицензии, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Продлить**.

Откроется веб-страница интернет-магазина «Лаборатории Касперского», где вы можете продлить срок действия лицензии.


КАК ОБНОВИТЬ БАЗЫ ПРОГРАММЫ

«Лаборатория Касперского» обновляет антивирусные базы Kaspersky Internet Security, используя серверы обновлений. Серверы обновлений «Лаборатории Касперского» – HTTP- и FTP-серверы «Лаборатории Касперского», на которые регулярно выкладываются обновления Kaspersky Internet Security.

Для успешной загрузки обновлений с серверов обновлений требуется подключение компьютера к интернету.

По умолчанию Kaspersky Internet Security периодически проверяет наличие обновлений на серверах обновлений «Лаборатории Касперского». Если на сервере содержится набор последних обновлений, Kaspersky Internet Security загружает их в фоновом режиме и устанавливает на компьютер.

► Чтобы запустить обновление Kaspersky Internet Security,

откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .

С результатами выполнения задачи обновления можно ознакомиться в окне отчетов.

КАК ЗАЩИТИТЬ ОТ ПЕРЕХВАТА ДАННЫЕ, ВВОДИМЫЕ С КЛАВИАТУРЫ

При работе в интернете часто возникают ситуации, когда необходимо указать персональные данные, а также имя пользователя и пароль. Это происходит, например, при регистрации на веб-сайтах, при совершении покупок в интернет-магазинах, при использовании интернет-банкинга.

В таких случаях существует опасность перехвата персональной информации с помощью программ, регистрирующих нажатие клавиш.

Виртуальная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

Виртуальная клавиатура не может защитить ваши персональные данные в случае взлома веб-сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников.

Виртуальная клавиатура защищает от перехвата персональной информации только при работе с веб-браузерами Safari, Firefox™ и Google Chrome™.

Виртуальная клавиатура имеет следующие особенности:

- На клавиши виртуальной клавиатуры нужно нажимать с помощью мыши.
- В отличие от настоящей клавиатуры, на виртуальной клавиатуре невозможно одновременно нажать несколько клавиш. Поэтому, чтобы ввести символ, который на настоящей клавиатуре вводится в комбинации с клавишами **ALT** и (или) **SHIFT**, нужно сначала нажать первую клавишу (например, **ALT**), а затем клавишу с изображением нужного символа.
- На виртуальной клавиатуре язык ввода переключается с помощью клавиши, расположенной в левом нижнем углу. Вы можете нажать на эту клавишу и выбрать в раскрывающемся списке язык ввода.

По умолчанию виртуальная клавиатура появляется на экране автоматически, если в окне веб-браузера выбрано поле для ввода пароля.

➤ *Чтобы открыть виртуальную клавиатуру,*

нажмите на кнопку  в панели инструментов веб-браузера.

КАК ОГРАНИЧИТЬ ВРЕМЯ РАБОТЫ ПОЛЬЗОВАТЕЛЯ В ИНТЕРНЕТЕ

Чрезмерно длительное нахождение детей и подростков за компьютером может нанести вред их здоровью. Если вам нужно ограничить время работы пользователя в интернете, вы можете воспользоваться категорией Контроль времени компонента Родительский контроль.

➤ *Чтобы ограничить время работы пользователя в интернете, выполните следующие действия:*

1. Откройте окно настройки Родительского контроля (на стр. [22](#)).
2. В левой части окна выберите учетную запись пользователя, для которого вы хотите ограничить время работы в интернете.
3. В правой части окна на закладке **Настройка** выберите категорию действий **Контроль времени**. Если контроль времени выключен, нужно его включить.
4. В блоке **Доступ в интернет за день** установите флажок **Максимальное время использования интернета**.
5. Перемещая ползунок, установите нужное количество часов в течение дня, когда доступ в интернет будет разрешен.
6. В блоке **Доступ в интернет в определенные часы** установите флажок **Разрешить доступ в интернет по дням недели**.
7. Задайте временные ограничения на использование интернета в будни и выходные дни.

С отчетом о попытках выхода пользователем в интернет в разрешенное и неразрешенное время вы можете ознакомиться на закладке **Отчеты** окна настройки Родительского контроля.

КАК ОГРАНИЧИТЬ ПОСЕЩЕНИЕ ВЕБ-САЙТОВ И ЗАГРУЗКУ ФАЙЛОВ ИЗ ИНТЕРНЕТА

Для обеспечения безопасности детей и подростков, использующих компьютер, вы можете ограничить следующие действия:

- посещение веб-сайтов, которые являются потенциальной причиной потери времени (чаты, игровые ресурсы) или денег (интернет-магазины, аукционы);
- доступ к веб-ресурсам, предназначенным для взрослой аудитории (например, содержащим порнографические, экстремистские материалы, затрагивающим темы оружия, наркотиков, насилия);
- загрузку некоторых типов файлов.

Вы можете воспользоваться категорией Веб-контроль компонента Родительский контроль.

➤ *Чтобы ограничить посещение веб-сайтов и загрузку файлов из интернета, выполните следующие действия:*

1. Откройте окно настройки Родительского контроля (на стр. [22](#)).
2. В левой части окна выберите учетную запись пользователя, для которого вы хотите ограничить доступ к веб-сайтам.
3. В правой части окна на закладке **Настройка** выберите категорию действий **Веб-контроль**. Если веб-контроль выключен, нужно его включить.
4. Установите флажок **Веб-контроль** и флажки для тех категорий веб-сайтов, доступ к которым нужно заблокировать.
5. Установите флажок **Контроль загружаемых файлов** и флажки для тех категорий файлов, загрузка которых разрешена.

При необходимости вы можете разрешить доступ к некоторым веб-сайтам, которые входят в категорию блокируемых, или запретить доступ к определенным веб-сайтам, сформировав список исключений.


С отчетом о попытках посещения заблокированных веб-сайтов и загрузки неразрешенных категорий файлов вы можете ознакомиться на закладке **Отчеты** окна настройки Родительского контроля.

КАК ОГРАНИЧИТЬ КОНТАКТЫ И ПЕРЕПИСКУ ПОЛЬЗОВАТЕЛЯ В СОЦИАЛЬНЫХ СЕТЯХ

Контроль контактов и переписки детей и подростков в социальных сетях позволяет предотвратить их контакты с незнакомыми людьми, которые под видом сверстников могут получить личную информацию о ребенке. Если у вас возникла необходимость ограничить контакты и переписку пользователя в социальных сетях, вы можете воспользоваться категорией Социальные сети компонента Родительский контроль.

➤ *Чтобы ограничить переписку через социальные сети, выполните следующие действия:*

1. Откройте окно настройки Родительского контроля (на стр. [22](#)).
2. В левой части окна выберите учетную запись пользователя, для которого вы хотите ограничить переписку через социальные сети.
3. В правой части окна на закладке **Настройка** выберите категорию действий **Социальные сети**. Если контроль социальных сетей выключен, нужно его включить.

4. Создайте список запрещенных и разрешенных контактов. Для этого нажмите на кнопку  и введите в поле в графе **Идентификатор** имя контакта в социальной сети (логин), а в поле в графе **Имя** – его реальное имя.

После добавления контакта в список Родительский контроль запрещает переписку с этим контактом в социальных сетях.

5. Если вы хотите временно разрешить переписку с контактом, выберите контакт в списке и снимите флажок в графе **Заблокирован**.

Переписка с этим контактом будет разрешена до тех пор, пока флажок не будет вновь установлен.

Если переписка с контактом запрещена, то Родительский контроль блокирует все сообщения, адресованные этому контакту или полученные от него.


На закладке **Отчеты** окна настройки Родительского контроля вы можете просмотреть следующую информацию:

- информацию о сообщениях, полученных или адресованных заблокированному контакту;
- информацию о наличии персональной информации в сообщениях;
- текст переписки с каждым контактом.

КАК ЗАПРЕТИТЬ ПЕРЕСЫЛКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Kaspersky Internet Security позволяет снизить риски, связанные с работой на компьютере и в интернете. Вы можете запретить пересылку данных, содержащих персональную информацию, через социальные сети и при отправке данных на веб-сайты с помощью категории Персональные данные компонента Родительский контроль.

➔ *Чтобы запретить пересылку персональных данных, выполните следующие действия:*

1. Откройте окно настройки Родительского контроля (на стр. [22](#)).
2. В левой части окна выберите учетную запись пользователя, для которого вы хотите запретить пересылку персональных данных.
3. В правой части окна на закладке **Настройка** выберите категорию действий **Персональные данные**. Если контроль персональных данных выключен, нужно его включить.
4. Создайте список персональных данных. Для этого нажмите на кнопку  и введите данные в поля в графах **Описание** и **Данные**. Например, вы можете создать записи для номера кредитной карты, домашнего адреса, номера телефона.


После добавления персональных данных в список Родительский контроль запрещает пересылку этих данных через социальные сети и отправку на веб-сайты.

Kaspersky Internet Security блокирует все попытки пересылки данных, добавленных в список. На закладке **Отчеты** окна настройки Родительского контроля вы можете просмотреть информацию о заблокированных сообщениях.

ЧТО ДЕЛАТЬ, ЕСЛИ ПРОГРАММА ЗАБЛОКИРОВАЛА ДОСТУП К ФАЙЛУ

Kaspersky Internet Security блокирует доступ к зараженным и возможно зараженным файлам или программам. Если файл заражен, для получения доступа его необходимо вылечить.

➤ Чтобы вылечить обнаруженные объекты, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .

Откроется окно отчетов Kaspersky Internet Security.

2. В левой части окна отчетов выберите **Обнаруженные объекты**.

В правой части окна в группе **Активные** отобразится список обнаруженных объектов с указанием их статуса. Вы можете раскрыть список объектов, нажав на значок ►.

3. Нажмите на кнопку **Лечить все**.

Программа начнет лечение обнаруженных объектов. Во время лечения объекта на экране отображается окно уведомления, в котором вы можете выбрать действие над объектом. Если после выбора действия над объектом вы установите в окне уведомления флажок **Применить во всех подобных случаях**, программа применит выбранное действие ко всем объектам этого типа.


Если вы уверены в безопасности объектов, доступ к которым блокируется Файловым Антивирусом, вы можете включить их в доверенную зону.

КАК ВОССТАНОВИТЬ УДАЛЕННЫЙ ИЛИ ВЫЛЕЧЕННЫЙ ПРОГРАММОЙ ОБЪЕКТ

Не рекомендуется без крайней необходимости восстанавливать удаленные и вылеченные объекты, поскольку они могут представлять угрозу для вашего компьютера.

Иногда в процессе лечения зараженных объектов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступной, можно попытаться восстановить исходный файл из его резервной копии.

➤ Чтобы восстановить удаленный или измененный при лечении объект, выполните следующие действия:

1. Откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .

Откроется окно отчетов Kaspersky Internet Security.

2. В левой части окна отчетов выберите **Карантин**.

В правой части окна отобразится содержимое карантина в виде списка резервных копий объектов.

3. Выберите резервную копию необходимого объекта в списке и нажмите на кнопку **Восстановить**. Подтвердите действие в открывшемся окне.


Объект будет восстановлен в исходное местоположение с тем же именем, которое было у него до лечения или удаления. Если в исходном местоположении уже находится объект с таким именем (эта ситуация возможна при восстановлении объекта, копия которого уже была создана перед лечением), на экране появится соответствующее предупреждение. Вы можете изменить местоположение восстанавливаемого объекта или переименовать его.

Рекомендуется сразу после восстановления проверить объект на вирусы. Возможно, с обновленными антивирусными базами объект удастся вылечить без потери целостности.

КАК ПРОСМОТРЕТЬ ОТЧЕТ О РАБОТЕ ПРОГРАММЫ

Информация о событиях, возникших в работе Файлового Антивируса, Веб-Антивируса, при выполнении задач поиска вирусов или обновления отображается в окне отчетов.

➡ Чтобы открыть окно отчетов,

откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку  .

ЧТО ДЕЛАТЬ ПРИ ПОЯВЛЕНИИ ОКОН УВЕДОМЛЕНИЙ И ВСПЛЫВАЮЩИХ СООБЩЕНИЙ

Уведомления программы (см. раздел «Окна уведомлений и всплывающие сообщения» на стр. [23](#)) в виде окон уведомлений информируют о событиях, происходящих во время работы программы и требующих вашего внимания.

При появлении на экране уведомления следует выбрать один из предложенных вариантов действия. Оптимальным вариантом действия является тот, который рекомендован специалистами «Лаборатории Касперского» по умолчанию.

РАБОТА С ПРОГРАММОЙ ИЗ КОМАНДНОЙ СТРОКИ

Вы можете работать с Kaspersky Internet Security посредством командной строки.

Синтаксис командной строки:

```
kav <команда> [параметры]
```

В качестве <команды> может использоваться:

- **help** – помощь по синтаксису команды, вывод списка команд;
- **scan** – проверка объектов на присутствие вредоносных программ;
- **update** – запуск обновления программы;
- **rollback** – откат последнего произведенного обновления Kaspersky Internet Security (для выполнения команды требуются права администратора компьютера);
- **start** – запуск компонента или задачи;
- **stop** – остановка работы компонента или задачи (для выполнения команды требуются права администратора компьютера);
- **status** – вывод на экран текущего статуса компонента или задачи;
- **statistics** – вывод на экран статистики по работе компонента или задачи;
- **export** – экспорт параметров компонента или задачи;
- **import** – импорт параметров компонента или задачи (для выполнения команды требуются права администратора компьютера);
- **addkey** – активация программы с помощью файла ключа (для выполнения команды требуются права администратора компьютера);
- **exit** – завершение работы программы (для выполнения команды требуются права администратора компьютера).

Каждой команде соответствует собственный набор параметров.

В ЭТОМ РАЗДЕЛЕ

Просмотр справки.....	48
Проверка на вирусы.....	48
Обновление программы.....	50
Откат последнего обновления.....	51
Запуск / остановка работы компонента или задачи.....	51
Статистика работы компонента или задачи.....	52
Экспорт параметров защиты.....	53
Импорт параметров защиты.....	53
Активация программы.....	53
Завершение работы программы.....	54
Коды возврата командной строки.....	54

ПРОСМОТР СПРАВКИ

Для просмотра справки по синтаксису командной строки предусмотрена команда:

```
kav [ -? | help ]
```

Для получения справки по синтаксису конкретной команды вы можете воспользоваться одной из следующих команд:

```
kav <команда> -?
kav help <команда>
```

ПРОВЕРКА НА ВИРУСЫ

Командная строка запуска проверки некоторой области на вирусы имеет следующий общий вид:

```
kav scan [<объект проверки>] [<действие>] [<типы файлов>] [<исключения>] [<параметры отчета>] [<дополнительные параметры>]
```

Для поиска вирусов вы также можете воспользоваться сформированными в программе задачами, запустив нужную из командной строки (см. раздел «Запуск / остановка работы компонента или задачи» на стр. [51](#)). При этом задача выполняется с параметрами, установленными в интерфейсе Kaspersky Internet Security.

Описание параметров

<объект проверки> – параметр задает перечень объектов, которые проверяются на присутствие вредоносного кода. Параметр может включать несколько значений из представленного списка, разделенных пробелом:

<files> – список путей к файлам и/или папкам для проверки. Допускается ввод абсолютного или относительного пути. Разделительный символ для элемента списка – пробел. Замечания:

- если имя объекта или путь содержит пробел или специальные символы (\$, &, @ и так далее), оно должно быть заключено в одинарные кавычки или исключаемый символ должен быть отделен с левой стороны обратной косой чертой;
- если указана конкретная папка, проверяются все файлы и папки, содержащиеся в ней.

-all – полная проверка компьютера;

-remdrives – все съемные диски;

-fixdrives – все локальные диски;

-netdrives – все сетевые диски;

-@:<filelist.lst> – путь к файлу со списком объектов и папок, включаемых в проверку. Файл должен иметь текстовый формат, каждый объект проверки требуется указывать с новой строки. Допускается ввод только абсолютного пути к файлу.

Если перечень объектов для проверки не указан, то Kaspersky Internet Security запускает задачу Поиск вирусов с параметрами, установленными в интерфейсе программы.

<действие> – параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению **-i8**. Возможны следующие значения:

-i0 – не совершать над объектом никаких действий, только сохранять информацию о нем в отчете;

-i1 – лечить зараженные объекты, если лечение невозможно – пропускать;

-i2 – лечить зараженные объекты, если лечение невозможно – удалять; не удалять контейнеры, кроме контейнеров с исполняемым заголовком (sfx-архивы);

-i3 – лечить зараженные объекты, если лечение невозможно – удалять; удалять контейнеры полностью, если невозможно удалить вложенные зараженные файлы;

-i4 – удалять зараженные объекты; удалять контейнеры полностью, если невозможно удалить вложенные зараженные файлы;

-i8 – запрашивать действие у пользователя при обнаружении зараженного объекта (используется по умолчанию);

-i9 – запрашивать действие у пользователя по окончании проверки.

<типы файлов> – параметр определяет типы файлов, которые подвергаются антивирусной проверке. По умолчанию, если параметр не задан, проверяются только заражаемые файлы по содержимому. Возможны следующие значения:

-fe – проверять только заражаемые файлы по расширению;

-fi – проверять только заражаемые файлы по содержимому (по умолчанию);

-fa – проверять все файлы.

<исключения> – параметр определяет объекты, исключаемые из проверки. Можно перечислить несколько параметров из следующего списка, разделив их пробелом:

-e:a – не проверять архивы;

-e:b – не проверять почтовые базы;

-e:m – не проверять почтовые сообщения в текстовом формате;

-e:<mask> – не проверять объекты по маске;

-e:<seconds> – пропускать объекты, которые проверяются дольше указанного времени в секундах;

-es:<size> – пропускать объекты, размер которых превышает указанное значение в мегабайтах.

<параметры отчета> – параметр определяет формат отчета о результатах проверки. Допускается использование абсолютного или относительного пути к файлу для сохранения отчета. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

-r:<report_file> – записывать в указанный файл отчета только важные события;

-ra:<report_file> – записывать в указанный файл отчета все события.

<дополнительные параметры> – параметры, определяющие использование технологий антивирусной проверки и файла настроек параметров:

-iSwift=<on|off> – включить / отключить использование технологии iSwift;

-c:<имя_конфигурационного_файла> – определяет путь к конфигурационному файлу, содержащему параметры работы программы при выполнении задач поиска вирусов. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, наряду со значениями уже указанными в командной строке, используются значения, установленные в интерфейсе программы.

Пример:

Запустить проверку папок ~/Documents, /Applications и файла my test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Проверить объекты, список которых приведен в файле object2scan.txt. Использовать для работы конфигурационный файл scan_settings.txt. По результатам проверки сформировать отчет, в котором зафиксировать все события:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Пример конфигурационного файла:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

ОБНОВЛЕНИЕ ПРОГРАММЫ

Команда для обновления программы имеет следующий синтаксис:

```
kav update [<источник_обновлений>] [-app=<on|off>] [<параметры_отчета>]
[<дополнительные_параметры>]
```

Описание параметров

<источник_обновлений> – HTTP-, FTP-сервер или сетевая или локальная папка для загрузки обновлений. Если путь не указан, источник обновлений будет взят из параметров сервиса обновления программы.

-app=<on|off> – включить / выключить обновление модулей программы.

<параметры отчета> – параметр определяет формат отчета о результатах проверки. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события. Возможны следующие значения:

-r:<report_file> – записывать в указанный файл отчета только важные события;

-ra:<report_file> – записывать в указанный файл отчета все события.

<дополнительные параметры> – параметр, определяющий использование файла настроек параметров.

-c:<имя_конфигурационного_файла> – определяет путь к конфигурационному файлу, содержащему параметры работы программы при выполнении обновления. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе программы.

Пример:

Обновить базы программы из источника по умолчанию, зафиксировав все события в отчете:

```
kav update -ra:avbases_upd.txt
```

Обновить модули Kaspersky Internet Security, используя параметры конфигурационного файла updateapp.ini:

```
kav update -app=on -c:updateapp.ini
```

ОТКАТ ПОСЛЕДНЕГО ОБНОВЛЕНИЯ

Синтаксис команды:

```
kav rollback [<параметры_отчета>]
```

Для выполнения команды требуются права администратора компьютера.

Описание параметров

<параметры отчета> – параметр, определяющий формат отчета о результатах отката обновления. Допускается использование абсолютного и относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

-r:<report_file> – записывать в указанный файл отчета только важные события;

-ra:<report_file> – записывать в указанный файл отчета все события.

Пример:

```
kav rollback -ra:rollback.txt
```

ЗАПУСК / ОСТАНОВКА РАБОТЫ КОМПОНЕНТА ИЛИ ЗАДАЧИ

Синтаксис команды start:

```
kav start <профайл|имя_задачи> [<параметры_отчета>]
```

Синтаксис команды stop:

```
kav stop <профайл|имя_задачи>
```

Для выполнения команды stop требуются права администратора компьютера.

Описание параметров

<параметры отчета> – параметр определяет формат отчета о результатах проверки. Допускается использование абсолютного и относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события. Возможны следующие значения:

-r:<report_file> – записывать в указанный файл отчета только важные события;

-ra:<report_file> – записывать в указанный файл отчета все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

<профайл|имя_задачи> – указывается одно из следующих значений:

file_monitoring (fm) – Файловый Антивирус;

web_monitoring (wm) – Веб-Антивирус;

scan_my_computer (full) – задача полной проверки компьютера;

scan_objects – проверка объектов;

scan_critical_areas (quick) - задача быстрой проверки компьютера;

updater – задача обновления;

rollback – задача отката обновлений.

Компоненты и задачи, запущенные из командной строки, выполняются с параметрами, установленными в интерфейсе программы.

Пример:

Чтобы включить Файловый Антивирус, в командной строке введите:

```
kav start fm
```

Чтобы остановить задачу полной проверки, в командной строке введите:

```
kav stop scan_my_computer
```

СТАТИСТИКА РАБОТЫ КОМПОНЕНТА ИЛИ ЗАДАЧИ

Синтаксис команды status:

```
kav status [<профайл|имя_задачи>]
```

Синтаксис команды statistics:

```
kav statistics <профайл|имя_задачи>
```

Описание параметров

<профайл|имя_задачи> – указывается одно из значений, перечисленных для команды start / stop (см. раздел «Запуск / остановка работы компонента или задачи» на стр. [51](#)).

Если команда `status` запускается без указания значения параметра **<профайл|имя_задачи>**, то на экран выводится текущий статус всех задач и компонентов программы. Для команды `statistics` значение параметра **<профайл|имя_задачи>** должно быть указано обязательно.

ЭКСПОРТ ПАРАМЕТРОВ ЗАЩИТЫ

Синтаксис команды:

```
kav export <профайл|имя_задачи> <имя_файла>
```

Описание параметров

<профайл|имя_задачи> – указывается одно из значений, перечисленных для команды `start / stop` (см. раздел «Запуск / остановка работы компонента или задачи» на стр. [51](#)).

<имя_файла> – путь к файлу, в который экспортируются параметры программы. Может быть указан абсолютный или относительный путь.

Пример:

```
kav export fm fm_settings.txt - текстовый формат
```

ИМПОРТ ПАРАМЕТРОВ ЗАЩИТЫ

Синтаксис команды:

```
kav import <имя_файла>
```

Для выполнения команды требуются права администратора компьютера.

Описание параметров

<имя_файла> – путь к файлу, из которого импортируются параметры программы. Может быть указан абсолютный или относительный путь.

Пример:

```
kav import settings.dat
```

АКТИВАЦИЯ ПРОГРАММЫ

Активацию Kaspersky Internet Security можно выполнить с использованием файла ключа.

Синтаксис команды:

```
kav addkey <имя_файла>
```

Для выполнения команды требуются права администратора компьютера.

Описание параметров

<имя_файла> – файл ключа к программе с расширением `key`.

Пример:

```
kav addkey 1AA111A1.key
```

ЗАВЕРШЕНИЕ РАБОТЫ ПРОГРАММЫ

Синтаксис команды:

```
kav exit
```

Для выполнения команды требуются права администратора компьютера.

КОДЫ ВОЗВРАТА КОМАНДНОЙ СТРОКИ

Общие коды могут быть возвращены любой командой командной строки. К кодам возврата задач относятся общие коды, а также коды, специфичные для конкретной задачи.

Общие коды возврата:

- 0 – операция выполнена успешно;
- 1 – неверное значение параметра;
- 2 – неизвестная ошибка;
- 3 – ошибка выполнения задачи;
- 4 – выполнение задачи отменено.

Коды возврата задач проверки на вирусы:

- 101 – все вредоносные объекты обработаны;
- 102 – обнаружены вредоносные объекты.

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	55
Техническая поддержка по телефону	55
Получение технической поддержки через Личный кабинет	56
Использование файла трассировки	57
Создание файла трассировки	57

СПОСОБЫ ПОЛУЧЕНИЯ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

- Чтобы просмотреть информацию о способах получения технической поддержки по Kaspersky Internet Security,

откройте главное окно программы (на стр. [20](#)) и нажмите на кнопку .

Если вы не нашли решения вашей проблемы в документации к программе или других источниках информации о программе, рекомендуется 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 международной Службы технической поддержки.
- Отправить запрос из Личного кабинета на веб-сайте Службы технической поддержки <https://my.kaspersky.com/>. 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 Вирусную 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 Вирусную лабораторию

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

Вы можете направлять запросы в Вирусную лабораторию в следующих случаях:

- если вы подозреваете, что файл или веб-ресурс содержит вирус, но Kaspersky Internet Security не обнаруживает наличие угроз. Специалисты Вирусной лаборатории анализируют присылаемый файл или веб-адрес и при обнаружении неизвестного ранее вируса добавляют информацию о нем в базу данных, доступную при обновлении антивирусных программ «Лаборатории Касперского»;
- если Kaspersky Internet Security определяет файл или веб-ресурс как содержащий вирус, но вы уверены, что файл или веб-ресурс не представляет угрозы.


Вы также можете направлять запросы в Вирусную 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.

ИСПОЛЬЗОВАНИЕ ФАЙЛА ТРАССИРОВКИ

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет с информацией об операционной системе и отправить его в Службу технической поддержки. Также специалисты Службы технической поддержки могут попросить вас создать *файл трассировки*. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

СОЗДАНИЕ ФАЙЛА ТРАССИРОВКИ

➔ Чтобы создать файл трассировки, выполните следующие действия:

1. Нажмите на кнопку  в главном окне программы (см. раздел «Главное окно программы» на стр. [20](#)).
Откроется окно настройки программы.
2. На закладке **Отчеты** окна настройки программы в блоке **Трассировка** установите флажок **Включить трассировку**.
3. Перезапустите Kaspersky Internet Security, чтобы запустить процесс трассировки.

Рекомендуется использовать эту опцию только под руководством специалиста Службы технической поддержки «Лаборатории Касперского».

Файлы трассировки могут занимать значительный объем дискового пространства. По окончании работы с файлами трассировки рекомендуется выключить их создание, сняв флажок **Включить трассировку** на закладке **Отчеты** окна настройки программы. После нужно перезапустить Kaspersky Internet Security.

ГЛОССАРИЙ

А

АКТИВАЦИЯ ПРОГРАММЫ

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

АКТИВНЫЙ КЛЮЧ

Ключ, используемый в текущий момент для работы программы.

Б

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.

БЛОКИРОВАНИЕ ОБЪЕКТА

Запрет доступа к объекту со стороны внешних программ. Заблокированный объект не может быть прочитан, выполнен или изменен.

В

ВОЗМОЖНО ЗАРАЖЕННЫЙ ОБЪЕКТ

Объект, код которого содержит модифицированный участок кода известной программы, представляющей угрозу, или объект, напоминающий такую программу по своему поведению.

ВОССТАНОВЛЕНИЕ

Перемещение оригинального объекта из карантина в папку его исходного расположения, где объект хранился до лечения или удаления, либо в другую папку, указанную пользователем.

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.

ЗАЩИТА

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект на чтение, запись и исполнение и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы или возможно зараженные, обрабатываются в соответствии с параметрами задачи (лечатся, удаляются, помещаются на карантин).

К

КАРАНТИН

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их первым лечением или удалением. Также на карантин программа «Лаборатории Касперского» помещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде, чтобы избежать их воздействия на компьютер.

Л**ЛЕЧЕНИЕ ОБЪЕКТОВ**

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

ЛОЖНОЕ СРАБАТЫВАНИЕ

Ситуация, когда незараженный объект определяется программой «Лаборатории Касперского» как зараженный из-за того, что его код напоминает код вируса.

О**ОБНОВЛЕНИЕ БАЗ**

Функция программы «Лаборатории Касперского», позволяющая поддерживать защиту компьютера в актуальном состоянии. Во время обновления программа копирует обновления баз и модулей программы с серверов обновлений «Лаборатории Касперского» на компьютер и автоматически устанавливает и применяет их.

Р**РЕЗЕРВНЫЙ КЛЮЧ**

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

С**СЕРВЕРЫ ОБНОВЛЕНИЙ «ЛАБОРАТОРИИ КАСПЕРСКОГО»**

HTTP-серверы и FTP-серверы «Лаборатории Касперского», с которых программы «Лаборатории Касперского» получают обновления баз и модулей программы.

СОСТОЯНИЕ ЗАЩИТЫ

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Т**ТЕХНОЛОГИЯ GROWL**

Универсальная система оповещения пользователя в операционной системе Mac OS X. Поддерживает всплывающие уведомления, голосовые уведомления, уведомления с помощью sms и email.

Внешний вид уведомлений, выводимых с помощью Growl, может быть настроен в разделе **Другие** панели Системные настройки, куда Growl автоматически встраивается после установки.

Э**ЭВРИСТИЧЕСКИЙ АНАЛИЗАТОР**

Технология обнаружения угроз, информация о которых еще не занесена в базы «Лаборатории Касперского». Эвристический анализатор позволяет обнаруживать объекты, поведение которых в системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

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 (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 файле `legal_notices.txt` (`file:///Library/Application%20Support/Kaspersky%20Lab/KAV/Doc/legal_notices.txt`), расположенном в папке установки программы.

УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Firefox – товарный знак Mozilla Foundation.

Google Chrome – товарный знак Google Inc.

Mac, Mac OS, Mountain Lion и Safari – зарегистрированные товарные знаки Apple Inc.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

К

Kaspersky Account 15, 16

А

Активация программы 31
 пробная версия 31
 с использованием кода активации 32

Б

Базы программы 41

В

Восстановление объекта 45

Г

Главное окно программы 20

З

Запуск
 задачи обновления 41
 задачи поиска вирусов 39, 40
Защита 36, 37

К

Карантин 45
Код активации 27

Л

Лицензия 25
 информация 29
 приобретение 29, 40
 продление 30, 41

О

Обновление программы 41
Отчеты 46

П

Подписка 30
Поиск вирусов 39, 40

Р

Родительский контроль 42, 43, 44

Т

Трассировка
 создание файла трассировки 57

У

Уведомления 23, 46

Ц

Центр защиты35, 37