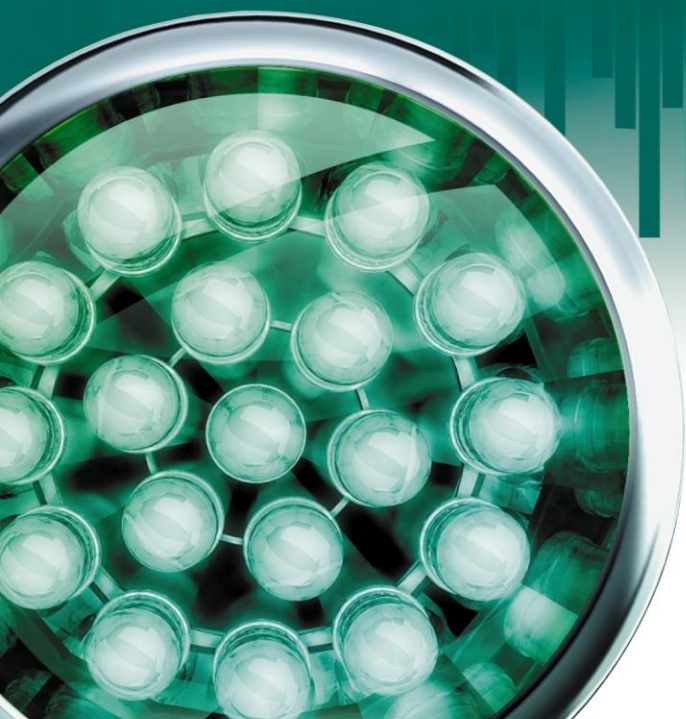


# Антивирус Касперского 6.0 для Windows Servers MP4

## РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ВЕРСИЯ ПРОГРАММЫ: 6.0 ПЛАНОВОЕ ОБНОВЛЕНИЕ 4, КРИТИЧЕСКОЕ  
ИСПРАВЛЕНИЕ 1



**KASPERSKY** lab

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» 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 законодательством Российской Федерации.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения ЗАО «Лаборатория 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, ЗАО «Лаборатория Касперского» ответственности не несет.

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

Дата редакции документа: 24.02.2010

© ЗАО «Лаборатория Касперского», 1997-2010

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

# СОДЕРЖАНИЕ

ВВЕДЕНИЕ .....	9
Комплект поставки .....	9
Лицензионное соглашение .....	9
Регистрационная карточка.....	10
Сервис для зарегистрированных пользователей.....	10
Аппаратные и программные требования к системе .....	10
АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS SERVERS MP4 .....	12
Получение информации о программе .....	12
Источники информации для самостоятельного поиска.....	12
Обращение в Департамент продаж .....	13
Обращение в Службу технической поддержки .....	13
Обсуждение программ «Лаборатории Касперского» на веб-форуме.....	14
Что нового в Антивирусе Касперского 6.0 для Windows Servers MP4 .....	14
На чем строится защита Антивируса Касперского .....	15
Файловый Антивирус .....	15
Задачи проверки на вирусы.....	16
Обновление .....	16
Сервисные функции программы .....	16
УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО 6.0 .....	18
Процедура установки с помощью мастера установки.....	18
Шаг 1. Проверка соответствия системы необходимым условиям установки Антивируса Касперского...	19
Шаг 2. Стартовое окно процедуры установки .....	19
Шаг 3. Просмотр Лицензионного соглашения .....	19
Шаг 4. Выбор каталога установки .....	19
Шаг 5. Использование параметров программы, сохраненных с предыдущей установки .....	20
Шаг 6. Выбор типа установки .....	20
Шаг 7. Выбор компонентов программы для установки.....	20
Шаг 9. Поиск других антивирусных программ .....	21
Шаг 10. Завершающая подготовка к установке программы .....	21
Шаг 11. Завершение процедуры установки.....	21
Процедура установки программы из командной строки .....	22
Процедура установки через Редактор объектов групповой политики (Group Policy Object) .....	22
Установка программы .....	22
Описание параметров файла setup.ini .....	23
Обновление версии программы .....	23
Удаление программы .....	24
НАЧАЛО РАБОТЫ .....	25
Мастер первоначальной настройки .....	25
Использование объектов, сохраненных с предыдущей версии.....	26
Активация программы .....	26
Онлайн-активация .....	27
Активация пробной версии .....	27
Активация с помощью файла ключа .....	27
Завершение активации .....	28

Настройка параметров обновления.....	28
Настройка расписания проверки на вирусы.....	28
Ограничение доступа к программе.....	29
Завершение работы мастера настройки.....	29
Проверка компьютера на вирусы.....	29
Обновление программы.....	30
Управление лицензиями.....	30
Управление безопасностью.....	31
Приостановка защиты.....	32
Устранение проблем. Техническая поддержка пользователей.....	33
Создание файла трассировки.....	33
Настройка параметров программы.....	34
Отчеты о работе программы. Файлы данных.....	34
ИНТЕРФЕЙС ПРОГРАММЫ.....	35
Значок в области уведомлений панели задач.....	35
Контекстное меню.....	36
Главное окно программы.....	37
Уведомления.....	38
Окно настройки параметров программы.....	39
АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВОЙ СИСТЕМЫ КОМПЬЮТЕРА.....	40
Алгоритм работы компонента.....	41
Изменение уровня безопасности.....	42
Изменение действия над обнаруженными объектами.....	42
Формирование области защиты.....	44
Использование эвристического анализа.....	45
Оптимизация проверки.....	45
Проверка составных файлов.....	45
Проверка составных файлов большого размера.....	46
Изменение режима проверки.....	46
Технология проверки.....	47
Приостановка работы компонента: формирование расписания.....	47
Приостановка работы компонента: формирование списка программ.....	48
Восстановление параметров защиты по умолчанию.....	48
Статистика защиты файлов.....	48
Отложенное лечение объектов.....	49
ПРОВЕРКА СЕРВЕРА НА ВИРУСЫ.....	50
Запуск проверки на вирусы.....	51
Формирование списка объектов проверки.....	53
Изменение уровня безопасности.....	53
Изменение действия при обнаружении угрозы.....	54
Изменение типа проверяемых объектов.....	55
Оптимизация проверки.....	55
Проверка составных файлов.....	56
Изменение метода проверки.....	57
Технология проверки.....	57
Производительность компьютера при выполнении задач.....	58
Приостановка задачи: формирование расписания.....	58
Приостановка работы компонента: формирование списка программ.....	59

Режим запуска: задание учетной записи.....	59
Режим запуска: формирование расписания .....	59
Особенности запуска задачи проверки по расписанию .....	60
Статистика проверки на вирусы.....	60
Назначение единых параметров проверки для всех задач .....	61
Восстановление параметров проверки по умолчанию .....	61
<b>ОБНОВЛЕНИЕ ПРОГРАММЫ.....</b>	<b>63</b>
Запуск обновления.....	64
Откат последнего обновления .....	65
Выбор источника обновлений .....	65
Региональные настройки.....	66
Использование прокси-сервера .....	66
Режим запуска: задание учетной записи.....	67
Режим запуска: формирование расписания .....	67
Выбор предмета обновления.....	68
Изменение режима запуска задачи обновления .....	68
Обновление из локальной папки .....	69
Статистика обновления .....	70
Возможные проблемы при обновлении .....	70
<b>НАСТРОЙКА ПАРАМЕТРОВ ПРОГРАММЫ .....</b>	<b>75</b>
<b>Защита .....</b>	<b>76</b>
Отключение / включение защиты компьютера.....	77
Запуск программы при старте операционной системы .....	77
Выбор категорий обнаруживаемых угроз .....	77
Формирование доверенной зоны .....	78
Создание правила исключения .....	78
Разрешенные маски исключений файлов.....	79
Разрешенные маски исключений по классификации Вирусной энциклопедии .....	80
Формирование списка доверенных программ .....	81
Экспорт / импорт компонентов доверенной зоны.....	81
Экспорт / импорт параметров работы Антивируса Касперского.....	82
Восстановление параметров по умолчанию .....	82
Файловый Антивирус .....	83
Проверка.....	83
Обновление .....	84
<b>Параметры.....</b>	<b>85</b>
Самозащита программы .....	85
Ограничение доступа к программе .....	86
Ограничение размера iSwift-файлов.....	86
Многопроцессорная конфигурация сервера .....	87
Уведомления о событиях Антивируса Касперского .....	87
Выбор типа события и способа отправки уведомлений .....	88
Настройка отправки уведомлений по электронной почте .....	88
Настройка параметров журнала событий.....	89
Активные элементы интерфейса .....	89
Отчеты и хранилища .....	90
Принципы работы с отчетами .....	90
Настройка параметров отчетов.....	91

Карантин возможно зараженных объектов.....	91
Действия с объектами на карантине.....	92
Резервные копии опасных объектов.....	92
Действия с резервными копиями .....	93
Настройка параметров карантина и резервного хранилища .....	93
ДИСК АВАРИЙНОГО ВОССТАНОВЛЕНИЯ.....	93
Создание диска аварийного восстановления .....	94
Шаг 1. Выбор источника образа диска.....	95
Шаг 2. Копирование (загрузка) образа диска .....	95
Шаг 3. Обновление файла образа .....	95
Шаг 4. Загрузка удаленного компьютера.....	96
Шаг 5. Завершение работы мастера.....	96
Загрузка компьютера с помощью диска аварийного восстановления .....	96
Работа с Kaspersky Rescue Disk из командной строки.....	99
Проверка на вирусы .....	100
Обновление Антивируса Касперского.....	101
Откат последнего обновления .....	102
Просмотр справки.....	102
ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ АНТИВИРУСА КАСПЕРСКОГО .....	103
Тестовый «вирус» EICAR и его модификации .....	103
Проверка корректности настройки Файлового Антивируса .....	104
Проверка корректности настройки задачи проверки на вирусы .....	105
ВИДЫ УВЕДОМЛЕНИЙ .....	106
Обнаружен вредоносный объект .....	106
Лечение объекта невозможно .....	107
Обнаружен подозрительный объект.....	107
РАБОТА С ПРОГРАММОЙ ИЗ КОМАНДНОЙ СТРОКИ .....	109
Просмотр справки .....	110
Проверка на вирусы.....	110
Обновление программы .....	112
Откат последнего обновления .....	113
Запуск / остановка работы Файлового Антивируса или задачи.....	113
Статистика работы компонента или задачи.....	114
Экспорт параметров защиты.....	115
Импорт параметров защиты.....	115
Активация программы.....	115
Восстановление файла из карантина.....	116
Завершение работы программы.....	116
Получение файла трассировки .....	116
Коды возврата командной строки .....	117
ИЗМЕНЕНИЕ, ВОССТАНОВЛЕНИЕ ИЛИ УДАЛЕНИЕ ПРОГРАММЫ.....	118
Изменение, восстановление и удаление программы с помощью мастера установки.....	118
Шаг 1. Стартовое окно программы установки .....	118
Шаг 2. Выбор операции.....	118
Шаг 3. Завершение операции восстановления, изменения или удаления программы .....	119
Удаление программы из командной строки .....	120

УПРАВЛЕНИЕ ПРОГРАММОЙ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT .....	121
Управление программой.....	123
Запуск и остановка программы .....	124
Настройка параметров программы .....	126
Настройка специфических параметров .....	127
Управление задачами.....	128
Запуск и остановка задач.....	130
Создание задачи .....	130
Мастер создания локальной задачи .....	131
Шаг 1. Ввод общих данных о задаче .....	131
Шаг 2. Выбор программы и типа задачи .....	131
Шаг 3. Настройка параметров выбранного типа задачи.....	132
Шаг 4. Настройка расписания .....	132
Шаг 5. Завершение создания задачи .....	132
Настройка параметров задач .....	132
Управление политиками.....	134
Создание политики.....	134
Мастер создания политики .....	135
Шаг 1. Ввод общих данных о политике .....	135
Шаг 2. Выбор статуса политики .....	135
Шаг 3. Импорт параметров программы.....	135
Шаг 4. Настройка параметров защиты.....	136
Шаг 5. Настройка защиты паролем .....	136
Шаг 6. Настройка доверенной зоны .....	136
Шаг 7. Настройка параметров взаимодействия с пользователем .....	136
Шаг 8. Завершение создания политики .....	136
Настройка параметров политики.....	137
ИСПОЛЬЗОВАНИЕ СТОРОННЕГО КОДА .....	139
Библиотека Boost-1.30.0.....	140
Библиотека LZMA SDK 4.40, 4.43 .....	140
Библиотека Windows Template Library 7.5.....	140
Библиотека Windows Installer XML (WiX) toolset 2.0 .....	141
Библиотека ZIP-2.31 .....	144
Библиотека ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3 .....	145
Библиотека UNZIP-5.51 .....	145
Библиотека LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12 .....	146
Библиотека LIBJPEG-6B.....	148
Библиотека LIBUNGIF-4.1.4 .....	150
Библиотека MD5 MESSAGE-DIGEST ALGORITHM-REV. 2.....	150
Библиотека MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004.....	150
Библиотека INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999 .....	150
Библиотека CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004.....	151
Библиотека COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum .....	151
Библиотека PLATFORM INDEPENDENT IMAGE CLASS .....	151
Библиотека FLEX PARSER (FLEXLEXER)-V. 1993.....	152
Библиотека ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 .....	152
Библиотека STDSTRING- V. 1999.....	153
Библиотека T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006 .....	153

Библиотека NTSERVICE- V. 1997 .....	154
Библиотека SHA-1-1.2 .....	154
Библиотека COCOA SAMPLE CODE- V. 18.07.2007 .....	155
Библиотека PUTTY SOURCES-25.09.2008.....	155
Другая информация .....	156
ГЛОССАРИЙ ТЕРМИНОВ .....	157
ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО» .....	164
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ .....	165



# ВВЕДЕНИЕ

## В ЭТОМ РАЗДЕЛЕ

---

Комплект поставки.....	<a href="#">9</a>
Сервис для зарегистрированных пользователей .....	<a href="#">10</a>
Аппаратные и программные требования к системе.....	<a href="#">10</a>

## КОМПЛЕКТ ПОСТАВКИ

Антивирус Касперского вы можете приобрести у наших партнеров (коробочный вариант), а также в одном из интернет-магазинов (например, <http://www.kaspersky.ru>, раздел **Интернет-магазин**).

Если вы приобретаете продукт в коробке, то в комплект поставки программного продукта входят:

- Запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта и документация в формате pdf.
- Руководство пользователя в печатном виде (если данная позиция была включена в заказ) или Руководство по продуктам.
- Файл ключа приложения, записанный на специальную дискету.
- Регистрационная карточка (с указанием серийного номера продукта).
- Лицензионное соглашение.

Перед тем как распечатать конверт с компакт-диском (или с дискетами), внимательно ознакомьтесь с лицензионным соглашением.

При покупке Антивируса Касперского в интернет-магазине вы копируете продукт с веб-сайта «Лаборатории Касперского», в дистрибутив которого помимо самого продукта включено также данное Руководство. Файл ключа будет вам отправлен по электронной почте по факту оплаты.

## ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО «Лаборатория Касперского», в котором указано, на каких условиях вы можете пользоваться приобретенным вами программным продуктом.

Внимательно прочитайте лицензионное соглашение!

Если вы не согласны с условиями лицензионного соглашения, вы можете вернуть коробку с продуктом партнеру, у которого она была приобретена, и получить назад сумму, уплаченную за продукт. При этом конверт с установочным компакт-диском (или с дискетами) должен оставаться запечатанным.

Открывая запечатанный пакет с установочным компакт-диском (или с дискетами), вы тем самым принимаете все условия лицензионного соглашения.

## РЕГИСТРАЦИОННАЯ КАРТОЧКА

Пожалуйста, заполните отрывной корешок регистрационной карточки, по возможности наиболее полно указав свои координаты: фамилию, имя, отчество (полностью), телефон, адрес электронной почты (если она есть), и отправьте ее дистрибьютору, у которого вы приобрели программный продукт.

Если впоследствии у вас изменится почтовый / электронный адрес или телефон, пожалуйста, сообщите об этом в организацию, куда был отправлен отрывной корешок регистрационной карточки.

Регистрационная карточка является документом, на основании которого вы приобретаете статус зарегистрированного пользователя нашей компании. Это дает вам право на техническую поддержку в течение срока действия лицензии. Кроме того, зарегистрированным пользователям, подписавшимся на рассылку новостей ЗАО «Лаборатория Касперского», высылается информация о выходе новых программных продуктов.

## СЕРВИС ДЛЯ ЗАРЕГИСТРИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

ЗАО «Лаборатория Касперского» предлагает своим легальным пользователям большой комплекс услуг, позволяющих увеличить эффективность использования приложения.

Приобретая лицензию, вы становитесь зарегистрированным пользователем и в течение срока действия лицензии можете получать следующие услуги:

- ежечасное обновление баз приложения и предоставление новых версий данного программного продукта;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией программного продукта, оказываемые по телефону и электронной почте;
- оповещение о выходе новых программных продуктов «Лаборатории Касперского» и о новых вирусах, появляющихся в мире. Данная услуга предоставляется пользователям, подписавшимся на рассылку новостей ЗАО «Лаборатория Касперского» на веб-сайте Службы технической поддержки (<http://support.kaspersky.ru/subscribe/>).

Консультации по вопросам функционирования и использования операционных систем, стороннего программного обеспечения, а также работы различных технологий не проводятся.

## АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ

Для нормального функционирования Антивируса Касперского 6.0, компьютер должен удовлетворять следующим минимальным требованиям:

*Общие требования:*

- 300 МБ свободного места на жестком диске.
- Microsoft Internet Explorer 6.0 или выше (для обновления баз и модулей программы через интернет).
- Microsoft Windows Installer 2.0 или выше.

*Windows 2000 Server / Advanced Server (Service Pack 4 Rollup1), Windows Server 2003 Standard / Enterprise (Service Pack 2), Windows Server 2003 x64 Standard / Enterprise (Service Pack 2), Windows Small Business Server 2003:*

- Процессор Intel Pentium 400 МГц 32-bit (x86) / 64-bit (x64) или выше (или совместимый аналог).
- 512 МБ свободной оперативной памяти.

*Windows Server 2003 R2 Standard / Enterprise Edition, Windows Server 2003 R2 x64 Standard / Enterprise Edition, Windows Server 2008 Standard / Enterprise (Service Pack 1 или выше), Windows Server 2008 x64 Standard / Enterprise (Service Pack 1 или выше), Windows Small Business Server 2008, Windows Essential Business Server 2008, Windows Server 2008 R2 x64 Standard / Enterprise:*

- Процессор Intel Pentium 1 ГГц 32-bit (x86) / 1,4 ГГц 64-bit (x64) или выше (или совместимый аналог).
- 1 ГБ свободной оперативной памяти.

# АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS SERVERS MP4

Антивирус Касперского 6.0 для Windows Servers MP4 – это новое поколение решений для защиты информации.

## В ЭТОМ РАЗДЕЛЕ

---

Получение информации о программе.....	12
Что нового в Антивирусе Касперского 6.0 для Windows Servers MP4 .....	14
На чем строится защита Антивируса Касперского.....	15

## ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ПРОГРАММЕ

Если у вас возникли вопросы, связанные с выбором, приобретением, установкой или использованием Антивируса Касперского, вы можете быстро получить ответы на них.

«Лаборатория Касперского» предоставляет различные источники информации о программе. Среди них вы можете выбрать наиболее удобный для себя в зависимости от важности и срочности вопроса.

## В ЭТОМ РАЗДЕЛЕ

---

Источники информации для самостоятельного поиска .....	12
Обращение в Департамент продаж .....	13
Обращение в Службу технической поддержки .....	13
Обсуждение программ «Лаборатории Касперского» на веб-форуме.....	14

## ИСТОЧНИКИ ИНФОРМАЦИИ ДЛЯ САМОСТОЯТЕЛЬНОГО ПОИСКА

Вы можете обратиться к следующим источникам информации о программе:

- странице программы на веб-сайте «Лаборатории Касперского»;
- странице программы на веб-сайте Службы технической поддержки (в Базе знаний);
- электронной справочной системе;
- документации.

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

[http://www.kaspersky.ru/anti-virus\\_windows\\_server](http://www.kaspersky.ru/anti-virus_windows_server) [http://www.kaspersky.ru/anti-virus\\_windows\\_server](http://www.kaspersky.ru/anti-virus_windows_server)

На этой странице вы получите общую информацию о программе, его возможностях и особенностях.

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

[http://support.kaspersky.ru/windows\\_file\\_server](http://support.kaspersky.ru/windows_file_server) [http://support.kaspersky.ru/windows\\_file\\_server](http://support.kaspersky.ru/windows_file_server)

На этой странице вы найдете статьи, опубликованные специалистами Службы технической поддержки.

Эти статьи содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы по приобретению, установке и использованию программы. Они сгруппированы по темам, таким как «Работа с файлами ключей», «Настройка обновлений баз» или «Устранение сбоев в работе». Статьи могут отвечать на вопросы, которые относятся не только к этой программе, но и к другим продуктам «Лаборатории Касперского»; они могут содержать новости Службы технической поддержки в целом.

### Электронная справочная система

В комплект поставки программы входит файл полной и контекстной справки, который содержит информацию о том, как управлять защитой компьютера: просматривать состояние защиты, проверять различные области компьютера на вирусы, выполнять другие задачи, а также информацию по каждому окну программы: перечень и описание представленных в нем параметров и список решаемых задач.

Чтобы открыть файл справки, нажмите на кнопку **Справка** в интересующем вас окне или на клавишу <F1>.

### Документация

В комплект поставки Антивируса Касперского входит документ **Руководство пользователя** (в формате .pdf). Данный документ содержит описание функций и возможностей программы и основные алгоритмы работы.

## ОБРАЩЕНИЕ В ДЕПАРТАМЕНТ ПРОДАЖ

Если у вас возникли вопросы по выбору, приобретению Антивируса Касперского или продлению срока его использования, вы можете поговорить с сотрудниками Департамента продаж в нашем центральном офисе в Москве по телефонам:

**+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00**

Обслуживание осуществляется на русском и английском языках.

Вы можете задать вопрос сотрудникам Департамента продаж по электронной почте, по адресу [sales@kaspersky.com](mailto:sales@kaspersky.com).

## ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Если вы уже приобрели Антивирус Касперского, вы можете получить информацию об этом приложении от специалистов Службы технической поддержки по телефону или через интернет.

Специалисты Службы технической поддержки ответят на ваши вопросы об установке и использовании приложения, а если ваш компьютер был заражен, они помогут устранить последствия работы вредоносных программ.

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

### Электронный запрос в Службу технической поддержки

Вы можете задать вопрос специалистам Службы технической поддержки, заполнив веб-форму системы обработки клиентских запросов Helpdesk (<http://support.kaspersky.ru/helpdesk.html>).

Вы можете отправить свой запрос на русском, английском, немецком, французском или испанском языках.

Чтобы отправить электронный запрос, вам нужно указать в нем **номер клиента**, полученный при регистрации на веб-сайте Службы технической поддержки, и **пароль**.

Если вы еще не являетесь зарегистрированным пользователем приложений «Лаборатории Касперского», вы можете заполнить регистрационную форму (<https://support.kaspersky.com/ru/personalcabinet/registration/form/>). При регистрации укажите код активации приложения или имя файла ключа.

Вы получите ответ на свой запрос от специалиста Службы технической поддержки в своем Персональном кабинете (<https://support.kaspersky.com/ru/PersonalCabinet>) и по электронному адресу, который вы указали в запросе.

В веб-форме запроса как можно подробнее опишите возникшую проблему. В обязательных для заполнения полях укажите:

- **Тип запроса.** Выберите тему, наиболее точно соответствующую возникшей проблеме, например «Проблема установки/удаления продукта» или «Проблема поиска/удаления вирусов». Если вы не найдете подходящей темы, выберите «Общий вопрос».
- **Название и номер версии приложения.**
- **Текст запроса.** Как можно подробнее опишите возникшую проблему.
- **Номер клиента и пароль.** Введите номер клиента и пароль, которые вы получили при регистрации на веб-сайте Службы технической поддержки.
- **Электронный адрес.** По этому адресу специалисты Службы технической поддержки перешлют ответ на ваш запрос.

### Техническая поддержка по телефону

Если проблема срочная, вы можете позвонить в Службу технической поддержки в вашем городе. Перед обращением к специалистам русскоязычной ([http://support.kaspersky.ru/support/support\\_local](http://support.kaspersky.ru/support/support_local)) или интернациональной (<http://support.kaspersky.ru/support/international>) технической поддержки, пожалуйста, соберите информацию (<http://support.kaspersky.ru/support/details>) о своем компьютере и установленном на нем антивирусном приложении. Это позволит нашим специалистам быстрее помочь вам.

## ОБСУЖДЕНИЕ ПРОГРАММ «ЛАБОРАТОРИИ КАСПЕРСКОГО» НА ВЕБ-ФОРУМЕ

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

На форуме вы можете просматривать опубликованные темы, оставлять свои комментарии, создавать новые темы, пользоваться поиском.

## ЧТО НОВОГО В АНТИВИРУСЕ КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS SERVERS MP4

Антивирус Касперского 6.0 – это универсальное средство защиты информации. Рассмотрим детально нововведения Антивируса Касперского 6.0.

### Новое в защите:

- Новое антивирусное ядро, на базе которого построен Антивирус Касперского, обладает более высокой эффективностью обнаружения вредоносных программ. Кроме того, новое антивирусное ядро обеспечивает существенное увеличение скорости проверки системы на присутствие вирусов. Это достигается за счет улучшенной обработки объектов и оптимизированного использования ресурсов компьютера (в особенности платформ на базе двух- и четырехъядерных процессоров).

- Реализован новый эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы. Если сигнатура программы не содержится в базах антивируса, эвристический анализатор имитирует ее запуск в изолированной виртуальной среде. Такой метод безопасен и позволяет проанализировать все действия программы еще до ее запуска в реальных условиях.
- Усовершенствована процедура обновления программы: теперь перезагрузка компьютера требуется в редких случаях.

#### *Новое в интерфейсе программы:*

- В интерфейсе реализован простой и удобный доступ к любому компоненту программы.
- Интерфейс разработан с учетом потребностей администраторов как небольших сетей, так и сетей крупных корпораций.

#### *Новое в работе через Kaspersky Administration Kit:*

- Kaspersky Administration Kit обеспечивает удобное и легкое управление системой антивирусной защиты организации. Программа способна централизованно управлять защитой корпоративной сети любого размера, насчитывающей десятки тысяч узлов, включая удаленных и мобильных пользователей.
- Реализована возможность удаленной установки программы с последней версией баз программы.
- Усовершенствован механизм работы с программой, установленной на удаленном компьютере (переработана структура политик).
- Реализована возможность использования конфигурационного файла программы при создании политики.
- При настройке параметров групповых задач обновления добавлена возможность устанавливать специфические параметры для мобильных пользователей.
- Реализована возможность временно выводить клиентские компьютеры с установленной программой из области действия политик и групповых задач (после ввода установленного пароля).

## НА ЧЕМ СТРОИТСЯ ЗАЩИТА АНТИВИРУСА КАСПЕРСКОГО

Защита включает:

- Файловый Антивирус (на стр. [15](#)), обеспечивающий контроль над объектами файловой системы компьютера в режиме реального времени.
- Задачи проверки на вирусы (на стр. [16](#)), посредством которых компьютер или отдельные файлы, папки, диски или области проверяются на присутствие вирусов.
- Обновление (на стр. [16](#)), обеспечивающее актуальность внутренних модулей программы, а также баз, используемых для поиска вредоносных программ.
- Сервисные функции (см. раздел «Сервисные функции программы» на стр. [16](#)), обеспечивающие информационную поддержку в работе с программой и позволяющие расширить ее функциональность.

## ФАЙЛОВЫЙ АНТИВИРУС

Защита сервера в реальном времени обеспечивается с помощью Файлового Антивируса.

Файловая система может содержать вирусы и другие опасные программы. Вредоносные программы могут годами храниться в вашей файловой системе, проникнув однажды со съемного диска или из интернета, и никак не проявлять себя. Однако стоит только открыть зараженный файл, вирус тут же проявит себя.

Файловый Антивирус – компонент, контролирующий файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается Антивирусом Касперского, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен программой. Если же файл по каким-либо причинам невозможно вылечить, он будет удален, при этом копия файла будет сохранена в резервном хранилище, или помещен на карантин.

## ЗАДАЧИ ПРОВЕРКИ НА ВИРУСЫ

Помимо защиты с помощью Файлового Антивируса, крайне важно периодически проводить проверку сервера на присутствие вирусов. Это необходимо делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены Файловым Антивирусом, например, из-за установленного низкого уровня защиты или по другим причинам.

Для проверки на вирусы в состав Антивируса Касперского включены следующие задачи:

### Проверка

Проверка объектов, выбранных пользователем. Вы можете проверить любой объект файловой системы компьютера.

### Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски.

### Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

## ОБНОВЛЕНИЕ

Чтобы всегда быть готовым уничтожить вирус или другую опасную программу, необходимо поддерживать Антивирус Касперского в актуальном состоянии. Для этого предназначен компонент **Обновление**. Он отвечает за обновление баз и модулей программы, используемых в работе программы.

Сервис копирования обновлений позволяет сохранять обновления баз, а также модулей программы, полученных с серверов «Лаборатории Касперского», в локальном каталоге, а затем предоставлять доступ к ним другим компьютерам сети в целях экономии интернет-трафика.

## СЕРВИСНЫЕ ФУНКЦИИ ПРОГРАММЫ

Антивирус Касперского включает ряд сервисных функций. Они предусмотрены для поддержки программы в актуальном состоянии, расширения возможностей использования программы, для оказания помощи в работе.

### Файлы данных

В процессе работы программы для каждого компонента защиты, задачи проверки на вирусы или обновления программы формируется отчет. Он содержит информацию о выполненных операциях и результаты работы, благодаря чему вы всегда сможете узнать подробности о работе любого компонента Антивируса Касперского. В случае возникновения проблем отчеты можно отправлять в «Лабораторию Касперского», чтобы наши специалисты смогли подробнее изучить ситуацию и как можно быстрее вам помочь.



Все подозрительные с точки зрения безопасности объекты Антивирус Касперского переносит в специальное хранилище – *Карантин*. Здесь они хранятся в зашифрованном виде, чтобы избежать заражения компьютера. Вы можете проверять эти объекты на присутствие вирусов, восстанавливать в исходном местоположении, удалять, самостоятельно добавлять объекты на карантин. Все объекты, которые по результатам проверки на вирусы окажутся незараженными, автоматически восстанавливаются в исходном местоположении.

В *Резервное хранилище* помещаются копии вылеченных и удаленных Антивирусом Касперского объектов. Данные копии создаются на случай необходимости восстановить объекты или картину их заражения. Резервные копии объектов также хранятся в зашифрованном виде, чтобы избежать заражения компьютера.

Вы можете восстановить объект из резервного хранилища в исходном местоположении или удалить копию.

### Диск восстановления

Диск аварийного восстановления предназначен для проверки и лечения зараженных x86-совместимых компьютеров. Он применяется при такой степени заражения, когда вылечить компьютер с помощью антивирусных программ или утилит лечения не представляется возможным.

### Лицензия

При покупке Антивируса Касперского между вами и «Лабораторией Касперского» заключается лицензионное соглашение, на основе которого вы можете использовать программу и получать доступ к обновлению баз программы и Службе технической поддержки в течение определенного периода. Срок использования, а также другая информация, необходимая для полноценной работы программы, указана в лицензии.

Пользуясь функцией **Лицензия**, вы можете получать подробную информацию об используемой вами лицензии, а также приобретать новую лицензию или продлевать действие текущей.

### Поддержка

Все зарегистрированные пользователи Антивируса Касперского могут воспользоваться Службой технической поддержки. Чтобы узнать о том, где именно вы можете получить техническую поддержку, воспользуйтесь функцией **Поддержка**.

С помощью соответствующих ссылок можно перейти на форум пользователей продуктов «Лаборатории Касперского», просмотреть список часто задаваемых вопросов, ответы на которые, возможно, помогут в решении вашей проблемы. Кроме того, заполнив, специальную форму на сайте, вы можете отправить в Службу технической поддержки сообщение об ошибке или отзыв о работе программы.

Вам также доступна Служба технической поддержки онлайн и, конечно, наши сотрудники всегда готовы вам помочь в работе с Антивирусом Касперского по телефону.

# УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО

## 6.0

Антивирус Касперского 6.0 для Windows Servers MP4 может быть установлен на компьютер несколькими способами:

- локальная установка – установка программы на отдельном компьютере. Для запуска и проведения установки требуется непосредственный доступ к данному компьютеру. Локальная установка может быть проведена в одном из двух режимов:
  - интерактивном, с помощью мастера установки программы (см. раздел «Процедура установки с помощью мастера установки» на стр. [18](#)), данный режим требует участия пользователя в процессе установки;
  - неинтерактивном, запуск установки программы в данном режиме выполняется из командной строки и не требует участия пользователя в процессе установки (см. раздел «Процедура установки программы из командной строки» на стр. [22](#)).
- удаленная установка – установка программы на компьютеры сети, выполняемая удаленно с рабочего места администратора с использованием:
  - программного комплекса Kaspersky Administration Kit (см. «Руководство по внедрению Kaspersky Administration Kit»);
  - групповых доменных политик Microsoft Windows Server 2000/2003 (см. раздел «Процедура установки через Редактор объектов групповой политики (Group Policy Object)» на стр. [22](#)).

Перед началом установки Антивируса Касперского (в том числе и удаленной) рекомендуется закрыть все работающие программы.

### В ЭТОМ РАЗДЕЛЕ

Процедура установки с помощью мастера установки .....	<a href="#">18</a>
Процедура установки программы из командной строки .....	<a href="#">22</a>
Процедура установки через Редактор объектов групповой политики (Group Policy Object).....	<a href="#">22</a>

## ПРОЦЕДУРА УСТАНОВКИ С ПОМОЩЬЮ МАСТЕРА УСТАНОВКИ

Чтобы установить Антивирус Касперского на ваш компьютер, на CD-диске с продуктом запустите файл дистрибутива.

Установка программы с дистрибутива, полученного через интернет, полностью совпадает с установкой программы с дистрибутивного CD-диска.

Программа установки выполнена в виде мастера. Каждое окно содержит набор кнопок для управления процессом установки. Кратко поясним их назначение:

- **Далее** – принять действие и перейти к следующему шагу процедуры установки.

- **Назад** – вернуться на предыдущий шаг установки.
- **Отмена** – отказаться от установки продукта.
- **Готово** – завершить процедуру установки программы на компьютер.

Рассмотрим подробно каждый шаг процедуры установки пакета.

## ШАГ 1. ПРОВЕРКА СООТВЕТСТВИЯ СИСТЕМЫ НЕОБХОДИМЫМ УСЛОВИЯМ УСТАНОВКИ АНТИВИРУСА КАСПЕРСКОГО

Перед установкой программы на компьютере выполняется проверка соответствия установленных операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки Антивируса Касперского. Также проверяется наличие на компьютере требуемых программ и ваши права на установку программного обеспечения.

В случае если какое-либо из требований не выполнено, на экран будет выведено соответствующее уведомление. Рекомендуется установить требуемые пакеты обновлений посредством сервиса **Windows Update** и необходимые программы перед установкой Антивируса Касперского.

## ШАГ 2. СТАРТОВОЕ ОКНО ПРОЦЕДУРЫ УСТАНОВКИ

Если ваша система полностью соответствует предъявляемым требованиям, сразу после запуска файла дистрибутива на экране будет открыто стартовое окно, содержащее информацию о начале установки Антивируса Касперского на компьютер.

Для продолжения установки нажмите на кнопку **Далее**. Отказ от установки продукта выполняется по кнопке **Отмена**.

## ШАГ 3. ПРОСМОТР ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ

Следующее окно программы установки содержит Лицензионное соглашение, которое заключается между вами и «Лабораторией Касперского». Внимательно прочтите его, и, при условии, что вы согласны со всеми пунктами соглашения, выберите вариант  **Я принимаю условия Лицензионного соглашения** и нажмите на кнопку **Далее**. Установка будет продолжена.

Для отказа от установки нажмите на кнопку **Отмена**.

## ШАГ 4. ВЫБОР КАТАЛОГА УСТАНОВКИ

Следующий этап установки Антивируса Касперского определяет каталог на компьютере, в который будет установлена программа. По умолчанию задан путь:

- **<Диск> → Program Files → Kaspersky Lab → Kaspersky Anti-Virus 6.0 для Windows Servers MP4** – для 32-разрядных систем.
- **<Диск> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 для Windows Servers MP4** – для 64-разрядных систем.

Вы можете указать другой каталог, нажав на кнопку **Обзор** и выбрав его в стандартном окне выбора каталога или введя путь к каталогу в соответствующем поле ввода.

Помните, если вы указываете полный путь к каталогу установки вручную, его длина не должна превышать 200 символов и содержать спецсимволы.

Для продолжения установки нажмите на кнопку **Далее**.

## ШАГ 5. ИСПОЛЬЗОВАНИЕ ПАРАМЕТРОВ ПРОГРАММЫ, СОХРАНЕННЫХ С ПРЕДЫДУЩЕЙ УСТАНОВКИ

На данном этапе вам будет предложено определить, хотите ли вы использовать в работе программы параметры защиты и базы программы, если таковые были сохранены на сервере при удалении предыдущей версии Антивируса Касперского 6.0.

Рассмотрим подробнее, как включить использование описанных выше возможностей.

Если на компьютере ранее была установлена предыдущая версия (сборка) Антивируса Касперского, и при ее удалении вы сохранили на компьютере базы программы, вы можете подключить их для использования в устанавливаемой версии. Для этого установите флажок  **Базы программы**. Базы, включенные в поставку программы, не будут копироваться на сервер.

Для того чтобы использовать параметры защиты, которые вы настроили в предыдущей версии и сохранили на компьютере, установите флажок  **Параметры работы программы**.

## ШАГ 6. ВЫБОР ТИПА УСТАНОВКИ

На данном этапе вам нужно определить полноту установки программы на ваш компьютер. Предусмотрено два варианта установки:

**Полная.** В этом случае все компоненты Антивируса Касперского будут установлены на сервер. Для ознакомления с дальнейшей последовательностью установки см. Шаг 8.

**Выборочная.** В данном случае вам будет предложено выбрать, какие компоненты программы вы хотите установить на сервер. Подробнее см. Шаг 7.

Для выбора типа установки нажмите на соответствующую кнопку.

## ШАГ 7. ВЫБОР КОМПОНЕНТОВ ПРОГРАММЫ ДЛЯ УСТАНОВКИ

Данный шаг выполняется только в случае **Выборочной** установки программы.

При выборочной установке вам нужно определить список компонентов Антивируса Касперского, которые вы хотите установить. По умолчанию для установки выбраны компонент Файловый Антивирус, компонент проверки на вирусы, а также коннектор к Агенту администрирования для удаленного управления программой через Kaspersky Administration Kit.

Для того чтобы выбрать компонент для последующей установки, нужно открыть меню по левой клавише мыши на значке рядом с именем компонента и выбрать пункт **Компонент будет установлен на локальный жесткий диск**. Подробнее о том, какую защиту обеспечивает выбранный компонент и сколько места на диске требуется для его установки, вы можете прочесть в нижней части данного окна программы установки.

Чтобы узнать подробную информацию о свободном месте на жестких дисках вашего компьютера, нажмите на кнопку **Диск**. Информация будет предоставлена в открывшемся окне.

Для отказа от установки компонента в контекстном меню выберите вариант **Компонент будет недоступен**. Помните, что, отменяя установку какого-либо компонента, вы лишаетесь защиты от целого ряда опасных программ.

После того как выбор устанавливаемых компонентов будет завершен, нажмите на кнопку **Далее**. Чтобы вернуться к списку устанавливаемых компонентов по умолчанию, нажмите на кнопку **Сброс**.

## ШАГ 9. ПОИСК ДРУГИХ АНТИВИРУСНЫХ ПРОГРАММ

На этом этапе осуществляется поиск других установленных на сервере антивирусных продуктов, в том числе и продуктов «Лаборатории Касперского», совместное использование с которыми Антивируса Касперского может привести к возникновению конфликтов.

При обнаружении таких программ на сервере их список будет выведен на экран. Вам будет предложено удалить их, прежде чем продолжить установку.

Под списком обнаруженных антивирусных программ вы можете выбрать, автоматически удалить их или ручную (автоматически будут удалены только продукты «Лаборатории Касперского»).

Для продолжения установки нажмите на кнопку **Далее**.

## ШАГ 10. ЗАВЕРШАЮЩАЯ ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММЫ

На данном этапе вам будет предложено произвести завершающую подготовку к установке программы на сервер.

При первоначальной установке Антивируса Касперского 6.0 не рекомендуется снимать флажок  **Защитить процесс установки**. Включенная защита модулей позволит, в случае возникновения ошибок в ходе установки программы, провести корректную процедуру отката установки. При повторной попытке установки программы рекомендуется снять данный флажок.

При удаленной установке программы на компьютер через **Windows Remote Desktop** рекомендуется снимать флажок  **Защитить процесс установки**. В противном случае процедура установки может быть не проведена или проведена некорректно.

Если вы хотите, чтобы в исключения автоматически были добавлены исключения, рекомендованные компанией Microsoft для серверов, установите флажок  **Исключить из антивирусной проверки области, рекомендованные компанией Microsoft**.

Если вы хотите, чтобы после установки в переменную окружения %Path% был добавлен путь к avr.com, установите флажок  **Добавить путь к avr.com к системной переменной %PATH%**.

Для продолжения установки нажмите на кнопку **Установить**.

В процессе установки в составе Антивируса Касперского компонентов, перехватывающих сетевой трафик, происходит разрыв текущих сетевых соединений. Большинство прерванных соединений восстанавливается через некоторое время.

## ШАГ 11. ЗАВЕРШЕНИЕ ПРОЦЕДУРЫ УСТАНОВКИ

Окно **Завершение установки** содержит информацию об окончании процесса установки Антивируса Касперского на компьютер.

Для запуска мастера первоначальной настройки программы нажмите на кнопку **Далее**.

Если для корректного завершения установки необходимо перезагрузить компьютер, на экран будет выведено соответствующее уведомление.

## ПРОЦЕДУРА УСТАНОВКИ ПРОГРАММЫ ИЗ КОМАНДНОЙ СТРОКИ

- Чтобы установить Антивируса Касперского 6.0 для Windows Servers MP4, наберите в командной строке:

```
msiexec /i <имя_пакета>
```

Будет запущен мастер установки (см. раздел «Процедура установки с помощью мастера установки» на стр. [18](#)). По завершении установки программы, необходимо перезагрузить компьютер.

- Чтобы установить программу в неинтерактивном режиме (без запуска мастера установки), наберите:

```
msiexec /i <имя_пакета> /qn
```

В данном случае по завершении установки программы потребуется вручную произвести перезагрузку компьютера. Для выполнения автоматической перезагрузки в командной строке наберите:

```
msiexec /i <имя_пакета> ALLOWREBOOT=1 /qn
```

Обратите внимание, что автоматическая перезагрузка компьютера может быть выполнена только в режиме неинтерактивной установки (с ключом /qn).

- Чтобы установить программу с указанием пароля, подтверждающего право на удаление программы, наберите:

```
msiexec /i <имя_пакета> KLUNINSTPASSWD=***** – при установке программы в интерактивном режиме;
```

```
msiexec /i <имя_пакета> KLUNINSTPASSWD=***** /qn – при установке программы в неинтерактивном режиме без перезагрузки компьютера;
```

```
msiexec /i <имя_пакета> KLUNINSTPASSWD=***** ALLOWREBOOT=1 /qn – при установке программы в неинтерактивном режиме с последующей перезагрузкой компьютера.
```

При установке Антивируса Касперского в неинтерактивном режиме поддерживается чтение файла setup.ini, содержащего общие параметры установки программы, конфигурационного файла *install.cfg* (см. раздел «Импорт параметров защиты» на стр. [115](#)), а также файла ключа. Обратите внимание, что данные файлы должны быть расположены в одном каталоге с дистрибутивом Антивируса Касперского.

## ПРОЦЕДУРА УСТАНОВКИ ЧЕРЕЗ РЕДАКТОР ОБЪЕКТОВ ГРУППОВОЙ ПОЛИТИКИ (GROUP POLICY OBJECT)

С помощью Редактора объектов групповой политики вы можете устанавливать, обновлять и удалять Антивирус Касперского на рабочих станциях предприятия, входящих в состав домена, без использования Kaspersky Administration Kit.

### УСТАНОВКА ПРОГРАММЫ

- Чтобы установить Антивирус Касперского, выполните следующие действия:

1. Создайте сетевую папку общего доступа на компьютере, являющемся контроллером домена, и поместите в нее дистрибутив Антивируса Касперского в формате *.msi*.

Дополнительно в данную директорию можно поместить файл *setup.ini*, содержащий перечень параметров установки Антивируса Касперского, конфигурационный файл *install.cfg* (см. раздел «Импорт параметров защиты» на стр. [115](#)), а также файл ключа.

- Откройте **Редактор объектов групповой политики** через стандартную консоль MMC (подробную информацию о работе с Редактором см. в справочной системе к Microsoft Windows Server).
- Создайте новый пакет. Для этого в дереве консоли выберите **Объект групповой политики / Конфигурация компьютера/ Конфигурация программ / Установка программного обеспечения** и воспользуйтесь командой **Создать / Пакет** контекстного меню.

В открывшемся окне укажите путь к сетевой папке общего доступа, содержащей дистрибутив Антивируса Касперского. В диалоговом окне **Развертывание программы** выберите параметр **Назначенный** и нажмите на кнопку **ОК**.

Групповая политика будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене. В результате Антивирус Касперского будет установлен на все компьютеры.

## ОПИСАНИЕ ПАРАМЕТРОВ ФАЙЛА SETUP.INI

Файл *setup.ini*, расположенный в каталоге дистрибутива Антивируса Касперского, используется при установке программы в неинтерактивном режиме через командную строку или Редактор объектов групповой политики. Данный файл содержит следующие параметры:

**[Setup]** – общие параметры установки программы.

- **InstallDir**=<путь к каталогу установки программы>.
- **Reboot=yes|no** – следует ли выполнять перезагрузку компьютера по завершении установки программы (по умолчанию перезагрузка не выполняется).
- **SelfProtection=yes|no** – следует ли включать самозащиту Антивируса Касперского при установке (по умолчанию самозащита включена).

**[Components]** – выбор компонентов программы для установки. В случае если данная группа не содержит элементов, программа устанавливается полностью.

- **FileMonitor=yes|no** – установка компонента Файловый Антивирус.

**[Tasks]** – включение задач Антивируса Касперского. В случае если не указана ни одна задача, после установки все задачи будут работать. Если указана хотя бы одна задача, все перечисленные задачи будут выключены.

- **ScanMyComputer=yes|no** – задача полной проверки.
- **ScanStartup=yes|no** – задача быстрой проверки.
- **Scan=yes|no** – задача проверки.
- **Updater=yes|no** – задача обновления баз и модулей программы.

Вместо значения **yes** могут использоваться значения 1, on, enable, enabled, а вместо значения **no** – 0, off, disable, disabled.

## ОБНОВЛЕНИЕ ВЕРСИИ ПРОГРАММЫ

➡ Чтобы обновить версию Антивируса Касперского, выполните следующие действия:

- Поместите дистрибутив, содержащий обновления Антивируса Касперского, в формате .msi в сетевую папку общего доступа.
- Откройте **Редактор объектов групповой политики** и создайте новый пакет описанным выше способом.

3. Выберите новый пакет в списке и воспользуйтесь командой **Свойства** контекстного меню. В окне свойств пакета перейдите на закладку **Обновления** и укажите пакет, который содержит дистрибутив предыдущей версии Антивируса Касперского. Чтобы установить обновленную версию Антивируса Касперского с сохранением параметров защиты, выберите вариант установки поверх существующего пакета.

Групповая политика будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене.

Обратите внимание, что на компьютерах с операционной системой Microsoft Windows 2000 Server не поддерживается обновление Антивируса Касперского через Редактор объектов групповой политики.

## УДАЛЕНИЕ ПРОГРАММЫ

➔ Чтобы удалить Антивирус Касперского, выполните следующие действия:

1. Откройте **Редактор объектов групповой политики**.
2. В дереве консоли выберите **Объект\_групповой\_политики / Конфигурация компьютера / Конфигурация программ / Установка программного обеспечения**.

В списке пакетов выберите пакет Антивируса Касперского, откройте контекстное меню и выполните команду **Все задачи / Удалить**.

В диалоговом окне **Удаление программ** выберите **Немедленное удаление этой программы с компьютеров всех пользователей**, чтобы Антивирус Касперского был удален при следующей перезагрузке компьютера.



# НАЧАЛО РАБОТЫ

Одной из главных задач специалистов «Лаборатории Касперского» при создании Антивируса Касперского являлась оптимальная настройка всех параметров программы.

Для удобства пользователей мы постарались объединить этапы предварительной настройки в едином интерфейсе мастера первоначальной настройки, который запускается в конце процедуры установки программы. Следуя указаниям мастера, вы сможете провести активацию программы, настроить параметры обновления и запуска задач проверки на вирусы, ограничить доступ к программе с помощью пароля.

После завершения установки и запуска программы на вашем компьютере мы рекомендуем вам выполнить следующие действия:

- Оценить текущий статус защиты (см. раздел «Управление безопасностью» на стр. [31](#)), чтобы убедиться, что Антивирус Касперского обеспечивает защиту на должном уровне.
- Обновить программу (см. раздел «Обновление программы» на стр. [30](#)) (если это не было сделано с помощью мастера настройки либо автоматически сразу после установки программы).
- Проверить сервер (см. раздел «Проверка компьютера на вирусы» на стр. [29](#)) на присутствие вирусов.

## В ЭТОМ РАЗДЕЛЕ

Мастер первоначальной настройки.....	<a href="#">25</a>
Проверка компьютера на вирусы .....	<a href="#">29</a>
Обновление программы .....	<a href="#">30</a>
Управление лицензиями .....	<a href="#">30</a>
Управление безопасностью .....	<a href="#">31</a>
Приостановка защиты .....	<a href="#">32</a>
Устранение проблем. Техническая поддержка пользователей .....	<a href="#">33</a>
Создание файла трассировки .....	<a href="#">33</a>
Настройка параметров программы .....	<a href="#">34</a>
Отчеты о работе программы. Файлы данных.....	<a href="#">34</a>

## МАСТЕР ПЕРВОНАЧАЛЬНОЙ НАСТРОЙКИ

Мастер настройки Антивируса Касперского запускается в конце процедуры установки программы. Его задача – помочь вам провести первичную настройку параметров программы, исходя из особенностей и задач вашего компьютера.

Интерфейс мастера настройки выполнен в стиле программы-мастера для Microsoft Windows (Windows Wizard) и состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Для полной установки программы на компьютер, необходимо выполнить все шаги мастера. Если по каким-либо причинам работа мастера была прервана, то уже заданные значения параметров не сохраняются. Далее, при

попытке начать работу с программой, мастер первоначальной настройки запускается вновь, что влечет за собой необходимость заново производить настройку параметров.

## ИСПОЛЬЗОВАНИЕ ОБЪЕКТОВ, СОХРАНЕННЫХ С ПРЕДЫДУЩЕЙ ВЕРСИИ

Данное окно мастера появляется при установке программы поверх предыдущей версии Антивируса Касперского. Вам предлагается выбрать, какие данные, используемые предыдущей версией, требуется перенести в новую версию. Это могут быть объекты карантина, резервного хранилища либо параметры защиты.

Для того чтобы использовать эти данные в новой версии программы, установите необходимые флажки.

## АКТИВАЦИЯ ПРОГРАММЫ

Процедура активации программы заключается в регистрации лицензии при помощи установки файла ключа. На основании лицензии программа будет определять наличие прав и срок на его использование.

Файл ключа содержит служебную информацию, необходимую для полнофункциональной работы Антивируса Касперского, а также дополнительные сведения:

- информацию о поддержке (кто осуществляет и где можно ее получить);
- название и номер ключа, а также дату окончания срока действия лицензии.

В зависимости от того, имеется ли у вас файл ключа или вам необходимо получить его с сервера «Лаборатории Касперского», вам предлагаются следующие варианты активации Антивируса Касперского:

- онлайн-активация (на стр. [27](#)). Выберите этот вариант активации, если вы приобрели коммерческую версию программы и вам был предоставлен код активации. На основании этого кода вы получите файл ключа, обеспечивающий доступ к полной функциональности программы на весь период действия лицензии.
- активация пробной версии (на стр. [27](#)). Выберите данный вариант активации, если вы хотите установить пробную версию программы перед принятием решения о покупке коммерческой версии. Вам будет предоставлен бесплатный файл ключа со сроком действия, ограниченным лицензией для пробной версии программы.
- активация с помощью полученного ранее файла ключа (см. раздел «Активация с помощью файла ключа» на стр. [27](#)). Активируйте программу с помощью полученного ранее файла ключа для Антивируса Касперского 6.0.
- активировать программу позже. При выборе этого варианта этап активации Антивируса Касперского будет пропущен. Программа будет установлена на ваш компьютер, вам будут доступны все функции программы, за исключением обновления (обновить программу вы сможете только один раз после установки). Вариант **Активировать программу позже** доступен только при первом запуске мастера активации. При последующих запусках мастера, в случае если программа уже активирована, вариант **Удалить файл ключа** для выполнения соответствующей операции.

При выборе первых двух вариантов активация программы осуществляется через веб-сервер «Лаборатории Касперского», для соединения с которым требуется подключение к интернету. Перед началом активации проверьте и, при необходимости, измените параметры сетевого соединения в окне, открываемом по кнопке **Параметры LAN**. Для получения более подробной информации о настройке сетевых параметров обратитесь к вашему системному администратору или интернет-провайдеру.

Если на момент установки соединение с интернетом отсутствует, вы можете провести активацию позже из интерфейса программы либо, выйдя в интернет с другого компьютера, получить файл ключа по коду активации, зарегистрировавшись на веб-сайте Службы технической поддержки «Лаборатории Касперского».

Вы также можете активировать программу через Kaspersky Administration Kit. Для этого необходимо создать задачу установки файла ключа (см. стр. [130](#)) (подробнее смотрите Справочное руководство «Kaspersky Administration Kit»).

## СМ. ТАКЖЕ

Онлайн-активация .....	<a href="#">27</a>
Получение файла ключа .....	<a href="#">27</a>
Активация с помощью файла ключа .....	<a href="#">27</a>
Завершение активации .....	<a href="#">28</a>

## ОНЛАЙН-АКТИВАЦИЯ

Онлайн-активация основана на вводе кода активации, который вы получаете по электронной почте при покупке Антивируса Касперского через интернет. В случае приобретения приложения в коробке код активации будет указан на конверте с установочным диском.

### Ввод кода активации

На данном этапе требуется указать код активации. Код активации представляет собой последовательность цифр, разделенных дефисами на четыре блока по пять символов, без пробелов. Например, 11111-11111-11111-11111. Обратите внимание, что код должен вводиться латинскими символами.

В нижней части окна укажите вашу контактную информацию: фамилию, имя, отчество, адрес электронной почты, страну и город проживания. Данная информация может потребоваться для идентификации зарегистрированного пользователя, если, например, данные о лицензии были утрачены или похищены. В данном случае на основании контактных данных вы сможете получить другой код активации.

### Получение файла ключа

Мастер настройки осуществляет соединение с серверами «Лаборатории Касперского» в интернете и отправляет на них ваши регистрационные данные (код активации, контактную информацию). После установления соединения на сервере проверяются код активации и полнота заполнения контактной информации. Если код активации прошел проверку, мастер получает файл ключа, который автоматически устанавливается. Процесс активации завершается, что сопровождается окном с подробной информацией о приобретенной лицензии.

Если код активации не прошел проверку, на экране появляется соответствующее уведомление. В данном случае вам следует обратиться за информацией в компанию, где вы приобрели Антивирус Касперского.

Если число активаций с помощью кода активации превышено, на экране также появляется соответствующее уведомление. Процесс активации будет прерван, и программа предложит вам обратиться в Службу поддержки «Лаборатории Касперского».

## АКТИВАЦИЯ ПРОБНОЙ ВЕРСИИ

Данный вариант активации следует использовать, если вы хотите установить пробную версию Антивируса Касперского перед принятием решения о покупке коммерческой версии. Вам будет предоставлена бесплатная лицензия со сроком действия, ограниченным лицензионным соглашением для пробной версии приложения. По истечении срока действия лицензии возможность повторной активации пробной версии будет недоступна.

## АКТИВАЦИЯ С ПОМОЩЬЮ ФАЙЛА КЛЮЧА

Если у вас уже есть файл ключа, вы можете активировать Антивирус Касперского с его помощью. Для этого воспользуйтесь кнопкой **Обзор** и выберите файл с расширением *.key*.

После успешной установки ключа в нижней части окна будет представлена информация о лицензии: номер лицензии, ее тип (коммерческая, пробная и т. д.), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

## ЗАВЕРШЕНИЕ АКТИВАЦИИ

Мастер настройки информирует вас об успешном завершении активации Антивируса Касперского. Кроме того, приводится информация о лицензии: номер лицензии, ее тип (коммерческая, для бета-тестирования, пробная и т.д.), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

## НАСТРОЙКА ПАРАМЕТРОВ ОБНОВЛЕНИЯ

Качество защиты вашего компьютера напрямую зависит от своевременного получения обновлений баз и модулей программы. В данном окне мастера настройки вам предлагается выбрать режим обновления программы и сформировать параметры расписания:

- **Автоматически.** Антивирус Касперского с заданной периодичностью проверяет наличие пакета обновлений в источнике обновления. Частота проверки может увеличиваться во время вирусных эпидемий и сокращаться вне их. При обнаружении свежих обновлений Антивирус Касперского скачивает их и устанавливает на компьютер. Такой режим используется по умолчанию.
- **Каждые 2 часа** (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию. Параметры расписания можно установить в окне, открываемом по кнопке **Изменить**.
- **Вручную.** В этом случае вы будете самостоятельно запускать обновление программы.

Обратите внимание, что базы и модули программы, входящие в дистрибутив, могут устареть на момент установки программы. Поэтому мы рекомендуем получить самые последние обновления программы. Для этого нажмите на кнопку **Обновить сейчас**. В данном случае Антивирус Касперского получит необходимый набор обновлений с сайтов обновления в интернете и установит их на компьютер.

Если вы хотите перейти к настройке параметров обновления (установить сетевые параметры, выбрать ресурс, с которого будет происходить обновление, настроить запуск обновления от имени определенной учетной записи, а также включить сервис копирования обновлений в локальный источник), нажмите на кнопку **Настройка**.

## НАСТРОЙКА РАСПИСАНИЯ ПРОВЕРКИ НА ВИРУСЫ

Поиск вредоносных объектов в заданных областях проверки – одна из важных задач, обеспечивающих защиту компьютера.

При установке Антивируса Касперского по умолчанию создаются три задачи проверки на вирусы. В данном окне мастера настройки вам предлагается выбрать режим запуска задач проверки:

### Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски. Параметры расписания можно изменить в окне, открываемом по кнопке **Изменить**.

### Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы. Параметры расписания можно изменить в окне, открываемом по кнопке **Изменить**.

## ОГРАНИЧЕНИЕ ДОСТУПА К ПРОГРАММЕ

Поскольку сервер могут использовать несколько человек, в том числе имеющих разные уровни компьютерной грамотности, а также в связи с тем, что вредоносные программы способны отключать защиту компьютера, вам предлагается ограничить доступ к Антивирусу Касперского с помощью пароля. Пароль позволяет защитить программу от попыток несанкционированного отключения защиты, изменения его параметров или удаления.

Для включения защиты установите флажок  **Включить защиту паролем** и заполните поля **Пароль** и **Подтверждение пароля**.

Ниже укажите область, на которую будет распространяться ограничение доступа:

- **Все операции (кроме уведомлений об опасности)**. Запрашивать пароль при иницировании любого действия пользователя с программой, за исключением работы с уведомлениями об обнаружении опасных объектов.
- **Отдельные операции:**
  - **Настройка параметров программы** – запрашивать пароль при попытке пользователя изменить параметры работы Антивируса Касперского.
  - **Завершение работы программы** – запрашивать пароль при попытке пользователя завершить работу программы.
  - **Отключение компонентов защиты и остановка задач проверки** – запрашивать пароль при попытке пользователя выключить работу Файлового Антивируса либо остановить задачу проверки на вирусы.
  - **Отключение политики Kaspersky Administration Kit** – запрашивать пароль при попытке пользователя вывести компьютер из области действия политик и групповых задач (при работе через Kaspersky Administration Kit).
  - **При удалении программы** – запрашивать пароль при попытке пользователя удалить программу с компьютера.

## ЗАВЕРШЕНИЕ РАБОТЫ МАСТЕРА НАСТРОЙКИ

В последнем окне мастера вы увидите сообщение о том, что установка и настройка Антивируса Касперского прошли успешно. Вы можете сразу запустить программу на выполнение, установив флажок  **Запустить программу**.

Если установка прошла некорректно, например, при обнаружении несовместимых версий других антивирусных программ, вам может быть предложено перезагрузить компьютер.

## ПРОВЕРКА КОМПЬЮТЕРА НА ВИРУСЫ

Разработчики вредоносного программного обеспечения предпринимают массу усилий для сокрытия деятельности своих программ, поэтому вы можете не заметить присутствия на вашем компьютере вредоносных программ.

На момент установки Антивируса Касперского автоматически выполняется задача **Быстрой проверки** компьютера. Эта задача направлена на поиск и нейтрализацию вредоносных программ в объектах, загружаемых при старте операционной системы.

Специалисты «Лаборатории Касперского» также рекомендуют выполнить задачу **Полной проверки** компьютера.

► *Чтобы запустить / остановить задачу проверки на вирусы, выполните следующие действия:*

1. Откройте главное окно программы.

2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Нажмите на кнопку **Выполнить проверку**, чтобы начать проверку. Нажмите на кнопку **Остановить проверку** во время работы задачи, если возникла необходимость остановить ее выполнение.

## ОБНОВЛЕНИЕ ПРОГРАММЫ

Для обновления Антивируса Касперского требуется наличие соединения с интернетом.

В поставку Антивируса Касперского включены базы, содержащие сигнатуры угроз. На момент установки программы базы могут устареть, так как «Лаборатория Касперского» регулярно обновляет базы и модули программы.

Во время работы мастера настройки программы можно выбрать режим запуска обновления. По умолчанию Антивирус Касперского автоматически проверяет наличие обновлений на серверах «Лаборатории Касперского». Если на сервере содержится набор последних обновлений, Антивирус Касперского в фоновом режиме скачивает и устанавливает их.

Для поддержания защиты сервера в актуальном состоянии рекомендуется обновить Антивирус Касперского непосредственно после установки.

➔ Чтобы самостоятельно обновить Антивирус Касперского, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на кнопку **Выполнить обновление**.

## УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ

Возможность использования Антивируса Касперского определяется наличием лицензии. Лицензия предоставляется вам на основании покупки продукта и дает право использовать программу со дня активации.

Без лицензии в случае, если не было активации пробной версии программы, Антивирус Касперского будет работать в режиме – одно обновление. В дальнейшем новые обновления производиться не будут.

Если была активирована пробная версия программы, то после завершения срока действия пробной лицензии, Антивирус Касперского работать не будет.

По окончании срока действия коммерческой лицензии функциональность программы сохраняется за исключением возможности обновления баз программы. Вы по-прежнему можете проверять ваш компьютер посредством задач проверки и использовать компоненты защиты, но только на основе баз, актуальных на дату окончания срока действия лицензии. Следовательно, мы не гарантируем вам стопроцентную защиту от новых вирусов, которые появятся после окончания действия ключа.

Чтобы избежать заражения вашего компьютера новыми вирусами, мы рекомендуем вам продлить лицензию на использование Антивируса Касперского. За две недели до истечения срока действия лицензии программа уведомляет вас об этом. В течение некоторого периода времени при каждом запуске программы на экран выводится соответствующее сообщение.

Основная информация об используемой лицензии (активной и дополнительной, если последняя была установлена) представлена в разделе **Лицензия** главного окна Антивируса Касперского: тип лицензии (коммерческая, пробная, для бета-тестирования), ограничение количества компьютеров, дата окончания срока действия лицензии и количество дней до этой даты. Чтобы получить более подробную информацию и лицензии, воспользуйтесь ссылкой с используемым типом лицензии.

Чтобы ознакомиться с условиями лицензионного соглашения на использование программы воспользуйтесь кнопкой **Прочсть лицензионное соглашение**.

Чтобы удалить лицензию нажмите на кнопку **Добавить / Удалить** и следуйте указаниям открывшегося мастера.

Регулярно «Лаборатория Касперского» проводит акции, позволяющие продлить лицензию на использование наших продуктов со значительными скидками. Следите за акциями на веб-сайте «Лаборатории Касперского» в разделе **Продукты** → **Акции и спецпредложения**.

➔ *Чтобы приобрести лицензию или продлить срок ее действия, выполните следующие действия:*

1. Приобретите новый файл ключа или код активации. Для этого воспользуйтесь кнопкой **Купить лицензию** (в случае если программа не было активировано) или **Продлить лицензию**. На открывшейся веб-странице вам будет предоставлена полная информация об условиях покупки ключа через интернет-магазин «Лаборатории Касперского» либо у партнеров компании. При покупке через интернет-магазин по факту оплаты на электронный адрес, указанный в форме заказа, вам будет отправлен файл ключа либо код активации программы.
2. Активируйте программу. Для этого воспользуйтесь кнопкой **Добавить / Удалить** в разделе **Лицензия** главного окна программы либо командой **Активация** контекстного меню программы. В результате будет запущен мастер активации.

## УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

О появлении проблем в защите компьютера сигнализирует статус защиты компьютера (см. раздел «Главное окно программы» на стр. [37](#)) посредством изменения цвета значка статуса защиты и панели, на которой он расположен. При возникновении проблем в защите рекомендуется немедленно устранить их.

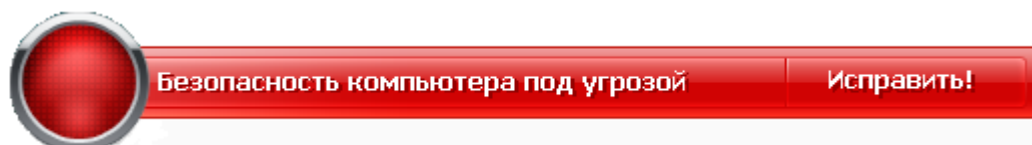


Рисунок 1. Текущее состояние защиты компьютера

Просмотреть список возникших проблем, их описание и возможные пути решения вы можете с помощью Мастера безопасности (см. рис. ниже), переход к которому осуществляется по ссылке [Исправить](#) (см. рис. выше).

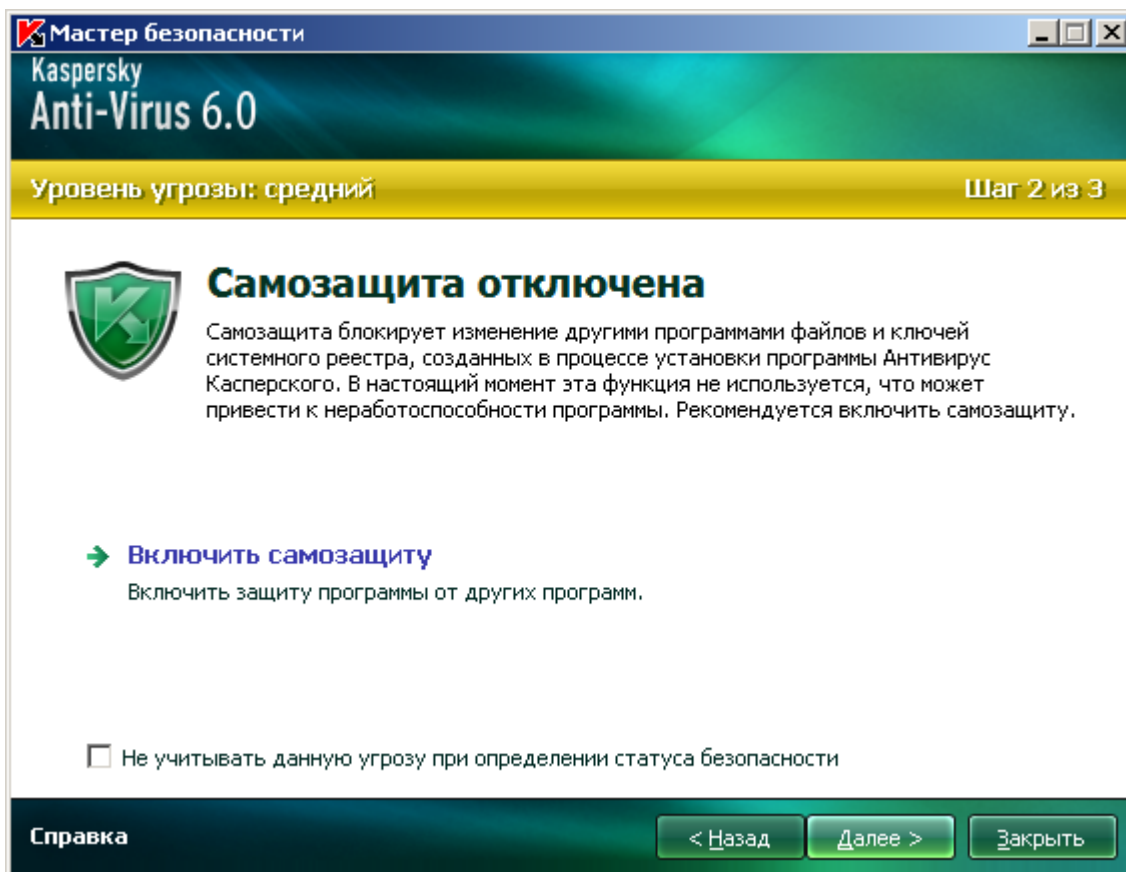


Рисунок 2. Решение проблем безопасности

Вы можете просмотреть список имеющихся проблем. Проблемы расположены исходя из важности их решения: сначала наиболее важные, то есть те, значок статуса которых красный; затем менее важные – значок статуса желтый, и последними – информационные сообщения. Для каждой проблемы дается ее подробное описание и предлагаются следующие варианты действий:

- *Немедленно устранить.* Используя соответствующие ссылки, вы можете перейти к непосредственному устранению проблемы, что является рекомендуемым действием.
- *Отложить устранение.* Если по какой-либо причине сиюминутное устранение проблемы невозможно, вы можете отложить данное действие и вернуться к нему позже. Установите флажок  **Не учитывать данную угрозу при определении статуса безопасности**, чтобы угроза не влияла на текущий статус защиты.

Обратите внимание, что для серьезных проблем данная возможность не предусмотрена. К ним относится, например, наличие необезвреженных вредоносных объектов, сбой в работе одного или нескольких компонентов, повреждение файлов программы. Такого рода проблемы необходимо устранять как можно быстрее.

## ПРИОСТАНОВКА ЗАЩИТЫ

Приостановка защиты означает отключение на некоторый промежуток времени Файлового Антивируса.

➔ *Чтобы приостановить работу Антивируса Касперского, выполните следующие действия:*

1. В контекстном меню программы выберите пункт **Приостановка защиты**.



2. В открывшемся окне **Приостановка защиты** из предложенных вариантов выберите время, спустя которое защита будет включена.

## УСТРАНЕНИЕ ПРОБЛЕМ. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ПОЛЬЗОВАТЕЛЕЙ

Если при использовании Антивируса Касперского возникли проблемы, прежде всего убедитесь, не описан ли метод решения вашей проблемы в справочной системе или в Базе знаний «Лаборатории Касперского» (<http://support.kaspersky.ru>). *База знаний* является отдельным разделом веб-сайта Службы технической поддержки и содержит рекомендации по работе с продуктами «Лаборатории Касперского», ответы на часто задаваемые вопросы. Попробуйте найти ответ на ваш вопрос или решение вашей проблемы на этом ресурсе.

► *Чтобы обратиться к Базе знаний, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна нажмите на ссылку **Поддержка**.
3. В открывшемся окне **Поддержка** нажмите на ссылку **Служба технической поддержки**.

Еще один ресурс, где вы можете получить информацию по работе с программой, – это Форум пользователей продуктов «Лаборатории Касперского». Данный ресурс также является отдельным разделом веб-сайта Службы технической поддержки и содержит вопросы, отзывы и пожелания пользователей программы. Вы можете ознакомиться с основными темами форума, оставить отзыв о программе или отыскать ответ на свой вопрос.

► *Чтобы открыть форум пользователей, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна нажмите на ссылку **Поддержка**.
3. В открывшемся окне **Поддержка** нажмите на ссылку **Форум пользователей**.

Если вы не нашли решения вашей проблемы в справке, Базе знаний или на Форуме пользователей, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского».

## СОЗДАНИЕ ФАЙЛА ТРАССИРОВКИ

После установки Антивируса Касперского могут возникнуть сбои в работе операционной системы или отдельных программ. В этом случае, скорее всего, имеет место конфликт программы с программным обеспечением, установленным на вашем компьютере, или с драйверами комплектующих вашего компьютера. Для успешного решения вашей проблемы специалисты Службы поддержки «Лаборатории Касперского» могут попросить вас создать файл трассировки.

► *Чтобы создать файл трассировки, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна программы нажмите на ссылку **Поддержка**.
3. В открывшемся окне **Поддержка** нажмите на ссылку **Трассировки**.
4. В открывшемся окне **Информация для поддержки** воспользуйтесь раскрывающимся списком в блоке **Трассировка**, чтобы выбрать уровень трассировки. Уровень трассировки задается специалистом Службы поддержки. При отсутствии указаний Службы поддержки рекомендуется устанавливать уровень трассировки **500**.
5. Чтобы запустить процесс трассировки, нажмите на кнопку **Включить**.

6. Воспроизведите ситуацию, в которой возникает ваша проблема.
7. Чтобы остановить процесс трассировки, нажмите на кнопку **Выключить**.

## НАСТРОЙКА ПАРАМЕТРОВ ПРОГРАММЫ

Для быстрого доступа к параметрам Антивируса Касперского 6.0 предназначено окно настройки параметров программы (см. стр. [75](#)), которое вызывается из главного окна с помощью кнопки **Настройка**.

## ОТЧЕТЫ О РАБОТЕ ПРОГРАММЫ. ФАЙЛЫ ДАННЫХ

Работа Файлового Антивируса и выполнение каждой задачи проверки и обновления фиксируется в отчете (см. стр. [90](#)). Чтобы перейти к просмотру отчетов, воспользуйтесь кнопкой **Отчеты**, расположенной в правом нижнем углу главного окна.

Объекты, помещенные в процессе работы Антивируса Касперского на карантин (см. стр. [91](#)) или в резервное хранилище (см. стр. [92](#)), называются *файлами данных программы*. С помощью кнопки **Обнаружено** вы можете открыть окно **Хранилище данных**, в котором можно выполнять над этими объектами нужные действия.

# ИНТЕРФЕЙС ПРОГРАММЫ

Антивирус Касперского обладает простым и удобным в работе интерфейсом. В данной главе мы подробнее рассмотрим основные его элементы:

- значок в системной панели;
- контекстное меню;
- главное окно;
- уведомления;
- окно настройки параметров Антивируса Касперского.

## В ЭТОМ РАЗДЕЛЕ



---

Значок в области уведомлений панели задач.....	<a href="#">35</a>
Контекстное меню.....	<a href="#">36</a>
Главное окно программы .....	<a href="#">37</a>
Уведомления.....	<a href="#">38</a>
Окно настройки параметров программы.....	<a href="#">39</a>




## ЗНАЧОК В ОБЛАСТИ УВЕДОМЛЕНИЙ ПАНЕЛИ ЗАДАЧ

Сразу после установки Антивируса Касперского в системной панели появляется его значок.

Значок является своего рода индикатором работы Антивируса Касперского. Он отражает состояние защиты, а также показывает ряд основных действий, выполняемых программой.

Если значок активный  (цветной), это означает, что защита сервера включена. Если значок неактивный  (черно-белый), значит, защита выключена.

В зависимости от выполняемой операции значок Антивируса Касперского меняется:

-  – выполняется проверка файла, который открываете, сохраняете или запускаете вы или некоторая программа.
-  – выполняется обновление баз и модулей Антивируса Касперского.
-  – произошел сбой в работе какого-либо из компонентов Антивируса Касперского.

Также значок обеспечивает доступ к основным элементам интерфейса программы: контекстному меню и главному окну.

Чтобы открыть контекстное меню, нажмите правой клавишей мыши на значок программы.

Чтобы открыть главное окно Антивируса Касперского, нажмите левой клавишей мыши на значок программы.

## КОНТЕКСТНОЕ МЕНЮ

Контекстное меню позволяет перейти к выполнению основных задач защиты.

Меню Антивируса Касперского содержит следующие пункты:

- **Полная проверка** – запуск полной проверки вашего компьютера на присутствие вредоносных объектов. В результате будут проверены объекты на всех дисках, в том числе и сменных носителях.
- **Проверка** – переход к выбору объектов и запуску проверки на вирусы. По умолчанию список содержит ряд объектов, например, системная память, объекты автозапуска, почтовые базы, все диски сервера и т. д. Вы можете пополнить список, выбрать объекты для проверки и запустить проверку на вирусы.
- **Обновление** – запуск обновления модулей и баз программы для Антивируса Касперского и их установка на вашем компьютере.
- **Активация** – переход к активации программы. Для получения статуса зарегистрированного пользователя, на основании которого вам будут доступны полная функциональность программы и сервисы Службы технической поддержки, необходимо активировать вашу версию Антивируса Касперского. Данный пункт меню присутствует только в том случае, если программа не активирована.
- **Настройка** – переход к просмотру и настройке параметров работы Антивируса Касперского.
- **Антивирус Касперского** – открытие главного окна программы.
- **Приостановка защиты / Включение защиты** – временное выключение / включение работы Файлового Антивируса. Данный пункт меню не влияет на обновление программы и на выполнение задач проверки.
- **Отключение политики / Включение политики** – временно выключение / включение политики при работе программы через Kaspersky Administration Kit. Пункт меню позволяет вывести компьютер из зоны действия политик и групповых задач. Данная возможность управляется паролем (см. раздел «Ограничение доступа к программе» на стр. [86](#)). Пункт меню появляется в том случае, если задан пароль.
- **О программе** – вызов информационного окна о программе.
- **Выход** – завершить работу Антивируса Касперского (при выборе данного пункта меню программа будет выгружена из оперативной памяти компьютера).

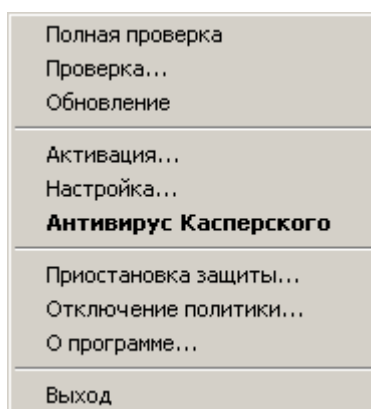


Рисунок 3. Контекстное меню

Если в данный момент запущена какая-либо задача проверки, ее имя будет отражено в контекстном меню с указанием результата выполнения в процентах. Выбрав задачу, вы можете перейти к окну отчета с текущими результатами ее выполнения.

## ГЛАВНОЕ ОКНО ПРОГРАММЫ

Главное окно программы можно условно разделить на три части:

- Верхняя часть окна сигнализирует о текущем состоянии защиты вашего компьютера.

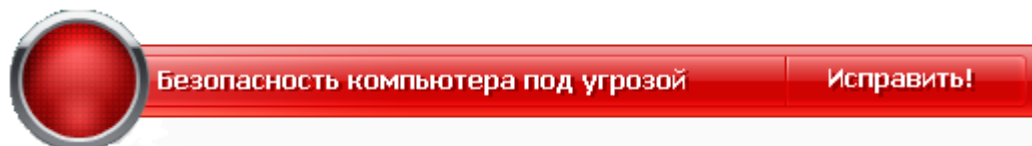


Рисунок 4. Текущее состояние защиты компьютера

Существует три возможных состояния защиты, каждое из которых выражено определенным цветом, аналогично сигналам светофора. Зеленый цвет говорит о том, что защита вашего компьютера осуществляется на должном уровне, желтый и красный цвета сигнализируют о наличии разного рода угроз безопасности в настройке параметров или работе Антивируса Касперского. К угрозам относятся не только вредоносные программы, но и, например, устаревшие базы программы.

По мере возникновения угроз безопасности их необходимо устранять. Для получения подробной информации о них и быстрого их устранения воспользуйтесь ссылкой **Исправить** (см. рис. выше).

- Левая часть окна позволяет быстро перейти к работе с любой функцией программы, к выполнению задач проверки на вирусы или обновления и др.

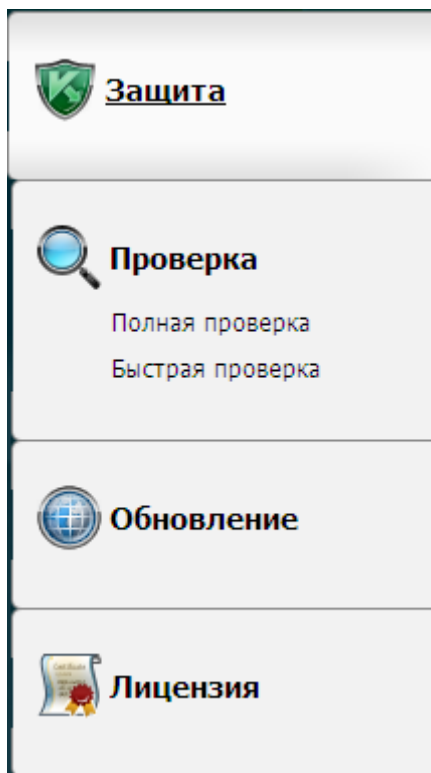


Рисунок 5. Левая часть главного окна

- Правая часть окна содержит информацию о выбранной в левой части функции программы, позволяет настроить параметры каждой из этих функций, предоставляет инструменты для выполнения задач проверки на вирусы, получения обновлений и т. д.

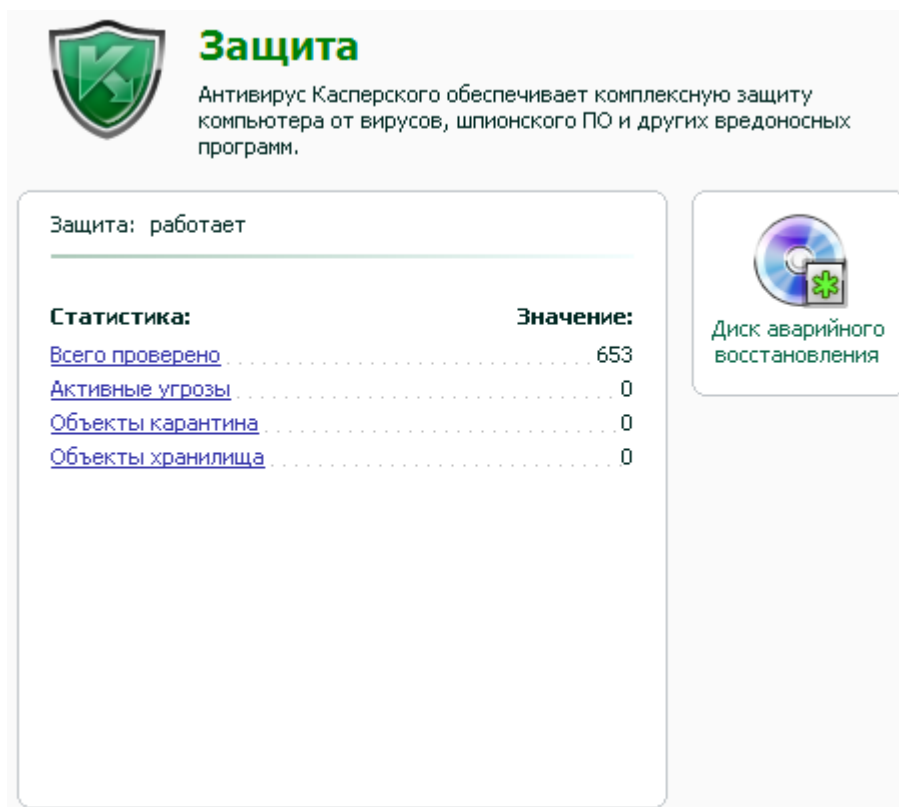


Рисунок 6. Правая часть главного окна

Кроме того, вы можете воспользоваться следующими инструментами:

- кнопкой **Настройка** – переход к окну настройки параметров программы (см. стр. [75](#));
- ссылкой **Справка** – переход к справочной системе Антивируса Касперского;
- кнопкой **Обнаружено** – переход к работе с файлами данных программы (см. стр. [90](#));
- кнопкой **Отчеты** – переход к отчетам о работе компонентов программы (см. стр. [90](#));
- ссылкой **Поддержка** – открытие окна с информацией о системе и ссылками на информационные ресурсы «Лаборатории Касперского» (см. стр. [33](#)) (сайт Службы технической поддержки, форум).

## УВЕДОМЛЕНИЯ

При возникновении событий в процессе работы Антивируса Касперского на экран выводятся специальные уведомления – всплывающие сообщения над значком программы в панели задач Microsoft Windows.

В зависимости от степени важности события, с точки зрения безопасности компьютера, уведомления могут быть следующих типов:

- **Тревога.** Произошло событие критической важности, например, обнаружен вирус. Необходимо немедленно принять решение о дальнейших действиях. Данный тип уведомления имеет красный цвет.

- **Внимание.** Произошло потенциально опасное событие, например, обнаружен возможно зараженный объект. Необходимо принять решение, насколько данное событие опасно на ваш взгляд. Данный тип уведомления имеет желтый цвет.
- **Информация.** Уведомление информирует о событии, не имеющем первостепенной важности. Информационные уведомления имеют зеленый цвет.

## СМ. ТАКЖЕ

---

Виды уведомлений ..... [106](#)

## ОКНО НАСТРОЙКИ ПАРАМЕТРОВ ПРОГРАММЫ

Окно настройки параметров Антивируса Касперского можно вызвать из главного окна. Для этого нажмите на кнопку **Настройка** в верхней его части.

Окно настройки построено аналогично главному окну:

- левая часть окна обеспечивает быстрый и удобный доступ к настройке Файлового Антивируса, задач проверки на вирусы, обновления, а также настройке сервисных функций программы;
- правая часть окна содержит непосредственно перечень параметров выбранного в левой части компонента Файловый Антивирус, задачи и т. д.

## СМ. ТАКЖЕ

---

Настройка параметров программы ..... [75](#)

# АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВОЙ СИСТЕМЫ КОМПЬЮТЕРА

**Файловый Антивирус** позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

По умолчанию Файловый Антивирус проверяет только новые или измененные файлы. Проверка файлов происходит с определенным набором параметров, который называется уровнем безопасности. При обнаружении угроз Файловый Антивирус выполняет заданное действие.

Уровень защиты файлов и памяти на вашем компьютере определяется следующими наборами параметров:

- параметры, формирующие защищаемую область;
- параметры, определяющие используемый метод проверки;
- параметры, определяющие проверку составных файлов (в том числе составных файлов больших размеров);
- параметры, задающие режим проверки;
- параметры, позволяющие приостановить работу компонента (по расписанию; во время работы выбранных программ).

► *Чтобы изменить параметры работы Файлового Антивируса, выполните следующие действия:*

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне внесите необходимые изменения в параметры компонента.



**В ЭТОМ РАЗДЕЛЕ**

Алгоритм работы компонента .....	<a href="#">41</a>
Изменение уровня безопасности .....	<a href="#">42</a>
Изменение действия над обнаруженными объектами .....	<a href="#">42</a>
Формирование области защиты .....	<a href="#">44</a>
Использование эвристического анализа .....	<a href="#">45</a>
Оптимизация проверки.....	<a href="#">45</a>
Проверка составных файлов .....	<a href="#">45</a>
Проверка составных файлов большого размера .....	<a href="#">46</a>
Изменение режима проверки.....	<a href="#">46</a>
Технология проверки.....	<a href="#">47</a>
Приостановка работы компонента: формирование расписания .....	<a href="#">47</a>
Приостановка работы компонента: формирование списка программ .....	<a href="#">48</a>
Восстановление параметров защиты по умолчанию.....	<a href="#">48</a>
Статистика защиты файлов .....	<a href="#">48</a>
Отложенное лечение объектов .....	<a href="#">49</a>

**АЛГОРИТМ РАБОТЫ КОМПОНЕНТА**

*Файловый Антивирус* запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

По умолчанию Файловый Антивирус проверяет только новые или измененные файлы, то есть файлы, которые были добавлены или изменены со времени последнего обращения к ним. Процесс проверки файла выполняется по следующему алгоритму:

1. Компонент перехватывает обращение пользователя или некоторой программы к каждому файлу.
2. Файловый Антивирус проверяет наличие информации о перехваченном файле в базах iChecker и iSwift и на основании полученной информации принимает решение о необходимости проверки файла.

Проверка включает следующие действия:

- Файл анализируется на присутствие вирусов. Распознавание объектов происходит на основании баз программы. Базы содержат описание всех известных в настоящий момент вредоносных программ, угроз, сетевых атак и способов их обезвреживания.
- В результате анализа возможны следующие варианты поведения Антивируса Касперского:
  - а. Если в файле обнаружен вредоносный код, Файловый Антивирус блокирует файл, помещает его копию в *резервное хранилище* и пытается провести лечение. В результате успешного лечения файл становится доступным для работы. Если же лечение провести не удалось, файл удаляется.

- b. Если в файле обнаружен код, похожий на вредоносный, но стопроцентной уверенности в этом нет, файл подвергается лечению и помещается в специальное хранилище – *карантин*.
- c. Если в файле не обнаружено вредоносного кода, он сразу же становится доступным для работы.

При обнаружении зараженного или возможно зараженного объекта программа уведомит вас об этом. Вам следует отреагировать на уведомление выбором действия:

- поместить угрозу на карантин для последующей проверки и обработки с помощью обновленных баз;
- удалить объект;
- пропустить, если вы абсолютно уверены, что данный объект не может являться вредоносным.

## СМ. ТАКЖЕ

Антивирусная защита файловой системы компьютера.....[40](#)

## ИЗМЕНЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ

Под уровнем безопасности подразумевается предустановленный набор параметров Файлового Антивируса. Специалистами «Лаборатории Касперского» сформированы три уровня безопасности. Решение о том, какой уровень выбрать, вы принимаете самостоятельно, в зависимости от условий работы и сложившейся ситуации.

- Если вероятность заражения компьютера очень высока, необходимо выбрать высокий уровень безопасности.
- Рекомендуемый уровень обеспечивает баланс между производительностью и безопасностью и подходит для большинства случаев.
- При работе в защищенной среде (например, в корпоративной сети с централизованным обеспечением безопасности), а также в случае работы с ресурсоемкими программами следует установить низкий уровень безопасности.

Перед включением низкого уровня безопасности рекомендуется провести полную проверку компьютера с высоким уровнем.

Если ни один из предложенных уровней не отвечает вашим требованиям, вы можете настроить параметры работы Файлового Антивируса. В результате название уровня безопасности изменится на **Другой**. Чтобы восстановить параметры работы компонента по умолчанию, выберите один из предустановленных уровней.

➔ *Чтобы изменить установленный уровень безопасности Файлового Антивируса, выполните следующие действия:*

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите нужный уровень безопасности.

## ИЗМЕНЕНИЕ ДЕЙСТВИЯ НАД ОБНАРУЖЕННЫМИ ОБЪЕКТАМИ

Файловый Антивирус в результате проверки присваивает найденным объектам один из следующих статусов:

- статус одной из вредоносных программ (например, *вирус, троянская программа*).

- *возможно зараженный*, когда в результате проверки однозначно невозможно определить, заражен объект или нет. Это означает, что в файле обнаружена последовательность кода неизвестного вируса или модифицированный код известного вируса.

Если в результате проверки файла на вирусы Антивирус Касперского находит зараженные или возможно зараженные объекты, дальнейшие операции Файлового Антивируса зависят от статуса объекта и выбранного действия.

По умолчанию все зараженные файлы подвергаются лечению, а все возможно зараженные – помещаются на карантин.

Все возможные действия приведены в таблице ниже.

Если в качестве действия вы выбрали	При обнаружении опасного объекта
<input checked="" type="checkbox"/> <b>Лечить</b> <input type="checkbox"/> <b>Удалить, если лечение невозможно</b>	Доступ к объекту блокируется и производится попытка его лечения, при этом копия объекта сохраняется в резервном хранилище. Если объект вылечить удалось, он предоставляется пользователю для работы. Если объект не удалось вылечить, то он помещается на карантин. Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.
<input checked="" type="checkbox"/> <b>Лечить</b> <input checked="" type="checkbox"/> <b>Удалить, если лечение невозможно</b>	Доступ к объекту блокируется и производится попытка его лечения, при этом копия объекта сохраняется в резервном хранилище. Если объект вылечить удалось, он предоставляется пользователю для работы. Если объект вылечить не удалось, то он будет удален.
<input type="checkbox"/> <b>Лечить</b> <input checked="" type="checkbox"/> <b>Удалить</b>	Файловый Антивирус блокирует доступ к объекту и удаляет его.
<input checked="" type="checkbox"/> <b>Блокировать пользователя на ... часов</b>	Заблокировать текущее подключение учетной записи пользователя к серверу при попытке копирования зараженного или возможно зараженного объекта.  Данное действие может быть применено дополнительно к действиям, связанным с обработкой объекта – лечению или удалению.  Обратите внимание, что если пользователь завершит сеанс работы и снова выполнит вход в систему, это будет расцениваться Антивирусом Касперского как другое подключение и блокировка будет снята.

Перед лечением или удалением объекта Антивирус Касперского формирует его резервную копию и помещает ее в резервное хранилище на тот случай, если понадобится восстановить объект или появится возможность его вылечить.

При статусе *возможно зараженный* объект помещается на карантин без попытки лечения.

➡ *Чтобы изменить установленное действие над обнаруженными объектами, выполните следующие действия:*

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне в блоке **Действие** выберите нужное действие.

## ФОРМИРОВАНИЕ ОБЛАСТИ ЗАЩИТЫ

Под областью защиты подразумевается не только местоположение проверяемых объектов, но и тип файлов, которые следует проверять. По умолчанию Антивирус Касперского проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков.

Вы можете расширить или сузить область защиты, путем добавления /удаления объектов проверки или изменения типа проверяемых файлов. Например, вы хотите проверять только exe-файлы, запускаемые с сетевых дисков. Однако вы должны быть уверены, что при сужении области защиты вы не подвергаете свой компьютер риску быть зараженным.

При выборе типа файлов следует помнить следующее:

- Существует ряд форматов файлов, для которых вероятность внедрения в них вредоносного кода и его последующей активации достаточно низка (например, *txt*). Существуют также форматы, которые содержат или могут содержать исполняемый код (*exe*, *dll*, *doc*). Риск внедрения в такие файлы вредоносного кода и его последующей активации достаточно высок.
- Злоумышленник может отправить вирус на ваш компьютер в файле с расширением *txt*, тогда как на самом деле это будет исполняемый файл, переименованный в *txt*-файл. Если выбран параметр **Файлы, проверяемые по расширению**, такой файл в процессе проверки будет пропущен. Если выбран параметр **Файлы, проверяемые по формату**, невзирая на расширение, Файловый Антивирус проанализирует заголовок файла, в результате чего выяснится, что файл имеет *exe*-формат. Такой файл будет подвергнут проверке на вирусы.

Указывая тип проверяемых файлов, вы определяете, файлы какого формата, размера и на каких дисках будут проверяться на присутствие вирусов при открытии, исполнении и сохранении.

Для простоты настройки все файлы разделены на две группы: *простые* и *составные*. Простые файлы не содержат в себе каких-либо объектов (например, *txt*-файл). Составные объекты могут включать несколько объектов, каждый из которых также может иметь несколько вложений. Примерами таких объектов могут служить архивы, файлы, содержащие в себе макросы, таблицы, письма с вложениями и т. д.

Помните, что Файловый Антивирус будет проверять на присутствие вирусов только те файлы, которые включены в сформированную область защиты. Файлы, не входящие в данную область, будут доступны для работы без проверки. Это повышает риск заражения компьютера!

➤ Чтобы изменить список проверяемых объектов, выполните следующие действия:

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Общие** в разделе **Область защиты** нажмите на кнопку **Добавить**.
4. В окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **Добавить**. После добавления всех нужных объектов нажмите на кнопку **ОК**.
5. Чтобы исключить какой-либо объект из списка проверки, снимите флажок рядом с ним.

➤ Чтобы изменить тип проверяемых файлов, выполните следующие действия:

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Общие** в блоке **Типы файлов** выберите нужный параметр.

## ИСПОЛЬЗОВАНИЕ ЭВРИСТИЧЕСКОГО АНАЛИЗА

По умолчанию проверка ведется на основе баз, содержащих описание известных угроз и методов лечения. Антивирус Касперского сравнивает найденный объект с записями в базах, в результате чего делается однозначный вывод о том, является ли проверяемый объект вредоносным, и к какому классу опасных программ он относится. Такой подход называется *сигнатурным анализом* и по умолчанию используется всегда.

В то же время каждый день появляются новые вредоносные объекты, записи о которых еще не попали в базы. Обнаружить такие объекты поможет эвристический анализ. Суть метода заключается в анализе активности, которую объект производит в системе. Если активность типична для вредоносных объектов, то с достаточной долей вероятности объект будет признан вредоносным или подозрительным. Следовательно, новые угрозы будут распознаны еще до того, как их активность станет известна вирусным аналитикам.

Дополнительно вы можете задать уровень детализации проверки. Уровень обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и временем проверки. Чем выше установленный уровень детализации проверки, тем больше ресурсов она потребует и больше времени займет.

► *Чтобы начать использовать эвристический анализ и задать уровень детализации проверки, выполните следующие действия:*

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Производительность** в блоке **Методы проверки** установите флажок  **Эвристический анализ** и ниже задайте уровень детализации проверки.

## ОПТИМИЗАЦИЯ ПРОВЕРКИ

Чтобы сократить время проверки и увеличить скорость работы Антивируса Касперского, вы можете проверять только новые файлы и те, что изменились с момента предыдущего их анализа. Этот режим работы распространяется как на простые, так и на составные файлы.

► *Чтобы проверять только новые файлы и те, что изменились с момента предыдущего анализа, выполните следующие действия:*

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Производительность** установите флажок  **Проверять только новые и измененные файлы**.

## ПРОВЕРКА СОСТАВНЫХ ФАЙЛОВ

Распространенная практика сокрытия вирусов предусматривает их внедрение в составные файлы: архивы, базы данных, и т. д. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать, что может привести к значительному снижению скорости проверки.

Установочные пакеты и файлы, содержащие OLE-объекты, исполняются при открытии, что делает их более опасными, чем архивы. Чтобы обезопасить свой компьютер от исполнения вредоносного кода и в то же время увеличить скорость проверки, отключите проверку архивов и включите проверку файлов данных типов.

Если файл, содержащий OLE-объект, представляет собой архив, он будет проверен при распаковке. Вы можете включить проверку архивов, чтобы проверять файлы, содержащие OLE-объекты, которые находятся в архиве, до его распаковки. Однако, это приведет к снижению скорости проверки.

По умолчанию Антивирус Касперского проверяет только вложенные OLE-объекты.

➤ *Чтобы изменить список проверяемых составных файлов, выполните следующие действия:*

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** установите флажки рядом с теми типами составных файлов, которые будут проверяться программой.

## ПРОВЕРКА СОСТАВНЫХ ФАЙЛОВ БОЛЬШОГО РАЗМЕРА

При проверке составных файлов большого размера их предварительная распаковка может занять много времени. Сократить это время можно, если проводить проверку файлов в фоновом режиме. Если во время работы с таким файлом будет обнаружен вредоносный объект, Антивирус Касперского уведомит вас об этом.

Вы можете снизить время доступа к составным файлам, отключив распаковку файлов, размер которых больше заданного. Проверка файлов при извлечении из архивов будет производиться всегда.

➤ *Чтобы программа распаковывала файлы больших размеров в фоновом режиме, выполните следующие действия:*

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.
4. В окне **Составные файлы** установите флажок  **Распаковывать составные файлы в фоновом режиме** и задайте значение минимального размера файла в поле ниже.

➤ *Чтобы программа не распаковывала составные файлы большого размера, выполните следующие действия:*

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.
4. В окне **Составные файлы** установите флажок  **Не распаковывать составные файлы большого размера** и задайте значение максимального размера файла в поле ниже.

## ИЗМЕНЕНИЕ РЕЖИМА ПРОВЕРКИ

Под режимом проверки подразумевается условие срабатывания Файлового Антивируса. По умолчанию программа использует интеллектуальный режим, когда решение о проверке объекта принимается на основе выполняемых с ним операций. Например, при работе с документом Microsoft Office программа проверяет файл при первом открытии и последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

Вы можете изменить режим проверки объектов. Выбор режима зависит от того, с какими файлами вы работаете большую часть времени.

➤ Чтобы изменить режим проверки объектов, выполните следующие действия:

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Дополнительно** в блоке **Режим проверки** выберите нужный режим.

## ТЕХНОЛОГИЯ ПРОВЕРКИ

Дополнительно вы можете задать технологию, которая будет использоваться Файловым Антивирусом:

- **iChecker**. Технология позволяет увеличить скорость проверки за счет исключения некоторых объектов. Исключение объекта из проверки осуществляется по специальному алгоритму, учитывающему дату выпуска баз программы, дату предыдущей проверки объекта, а также изменение параметров проверки.

Например, у вас есть файл архива, которому по результатам проверки программой был присвоен статус *не заражен*. В следующий раз этот архив будет исключен из проверки, если он не был изменен, и если не менялись параметры проверки. Если вы изменили состав архива, добавив в него новый объект, изменили параметры проверки, обновили базы программы, архив будет проверен повторно.

Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к объектам с известной программе структурой (например, файлы exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift**. Технология представляет собой развитие технологии iChecker для компьютеров с файловой системой NTFS. Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе и применима только к объектам, расположенным в файловой системе NTFS.

➤ Чтобы изменить технологию проверки объектов, выполните следующие действия:

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Дополнительно** в блоке **Технологии проверки** выберите нужное значение параметра.

## ПРИОСТАНОВКА РАБОТЫ КОМПОНЕНТА: ФОРМИРОВАНИЕ РАСПИСАНИЯ

При выполнении работ, требующих значительных ресурсов операционной системы, вы можете временно останавливать работу Файлового Антивируса. Чтобы снизить нагрузку и обеспечить быстрый доступ к объектам, можно настроить отключение компонента в определенное время.

➤ Чтобы настроить расписание приостановки работы компонента, выполните следующие действия:

1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок  **По расписанию** и нажмите на кнопку **Расписание**.
4. В окне **Приостановка задачи** укажите время (в формате ЧЧ:ММ), в течение которого защита будет приостановлена (поля **Приостановить в** и **Возобновить в**).

## ПРИОСТАНОВКА РАБОТЫ КОМПОНЕНТА: ФОРМИРОВАНИЕ СПИСКА ПРОГРАММ

При выполнении работ, требующих значительных ресурсов операционной системы, вы можете временно останавливать работу Файлового Антивируса. Чтобы снизить нагрузку и обеспечить быстрый доступ к объектам, можно настроить отключение компонента при работе с определенными программами.

**Настройка отключения Файлового Антивируса при конфликте с определенными программами – экстренная мера! В случае возникновения конфликтов при работе компонента обратитесь в Службу технической поддержки «Лаборатории Касперского» (<http://support.kaspersky.ru>). Специалисты поддержки помогут вам наладить совместную работу Антивируса Касперского с программами, установленными на вашем компьютере.**

- *Чтобы настроить приостановку компонента на время работы указанных программ, выполните следующие действия:*
1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
  2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **Настройка**.
  3. В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок  **При запуске программ** и нажмите на кнопку **Выбрать**.
  4. В окне **Программы** сформируйте список программ, при работе которых работа компонента будет приостановлена.

## ВОССТАНОВЛЕНИЕ ПАРАМЕТРОВ ЗАЩИТЫ ПО УМОЛЧАНИЮ

Настраивая работу Файлового Антивируса, вы всегда можете вернуться к рекомендуемым параметрам его работы. Они считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Если при настройке параметров Файлового Антивируса вы изменяли список объектов, включенных в область защиты, то при восстановлении первоначальных настроек вам будет предложено сохранить данный список для дальнейшего использования.

- *Чтобы восстановить параметры защиты по умолчанию, а также сохранить измененный список объектов, включенных в область защиты, выполните следующие действия:*
1. Откройте главное окно программы и в верхней части окна нажмите на кнопку **Настройка**.
  2. В открывшемся окне выберите компонент **Файловый Антивирус** и нажмите на кнопку **По умолчанию**.
  3. В открывшемся окне **Восстановление параметров** установите флажок  **Область защиты**.

## СТАТИСТИКА ЗАЩИТЫ ФАЙЛОВ

Все операции, производимые Файловым Антивирусом, фиксируются в специальном отчете. Чтобы ознакомиться с информацией о работе компонента, воспользуйтесь ссылкой **Статистика**. Вашему вниманию будет предоставлен детальный отчет о работе компонента, сгруппированный на закладках:

- Все опасные объекты, обнаруженные в процессе защиты файловой системы, перечислены на закладке **Обнаружено**. Здесь приводится полный путь к местоположению каждого объекта и статус, присвоенный объекту Файловым Антивирусом: если удалось точно установить, какой вредоносной программой



поражен объект, ему присваивается соответствующий статус. Например, вирус, троянская программа и т.д. Если тип вредоносного воздействия точно установить невозможно, объекту присваивается статус *подозрительный*. Рядом со статусом также указывается действие, выполненное над объектом (обнаружен, не найден, вылечен).

Чтобы данная закладка не содержала информации о вылеченных объектах, снимите флажок  **Показывать вылеченные объекты.**

- Полный список событий, возникших в работе Файлового Антивируса, ведется на закладке *События*. События могут быть следующих статусов:
  - *Информационное событие* (например: объект не обработан: пропущен по типу).
  - *Внимание* (например: обнаружен вирус).
  - *Примечание* (например: архив защищен паролем).

Как правило, информационные сообщения носят справочный характер и не представляют особого интереса. Вы можете отключить просмотр информационных сообщений. Для этого снимите флажок  **Показывать все события.**

- *Статистика* проверки приводится на соответствующей закладке. Здесь указывается общее количество проверенных объектов, а затем в специальных столбцах отдельно отражено, сколько объектов из общего числа проверенных являются архивами, сколько из них опасных объектов, сколько вылеченных, сколько помещенных на карантин и т.д.
- *Параметры*, в соответствии с которыми работает Файловый Антивирус, приводятся на одноименной закладке. Чтобы быстро перейти к настройке компонента, воспользуйтесь ссылкой **Изменить параметры**.
- Закладка *Заблокированные пользователи* отображает список пользователей, компьютеры которых были заблокированы при попытке произвести копирование зараженного или возможно зараженного объекта на сервер.

## ОТЛОЖЕННОЕ ЛЕЧЕНИЕ ОБЪЕКТОВ

В Антивирусе Касперского для Windows Servers MP4 доступ к зараженным объектам блокируется в случае лечения, если лечение не удалось, или удаления.

Чтобы вновь получить доступ к заблокированным объектам, необходимо предварительно попытаться вылечить их. Если объект удастся вылечить, он будет доступен для работы. Если вылечить объект нельзя, вам на выбор будет предложено *удалить* его или *пропустить*. В последнем случае доступ к файлу будет предоставлен. Однако это значительно повышает риск заражения сервера. Настоятельно не рекомендуется пропускать вредоносные объекты.

► *Чтобы получить доступ к заблокированным объектам с целью их лечения, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Обнаружено**.
2. В открывшемся окне на закладке **Активные угрозы** выберите интересующие вас объекты и нажмите на ссылку **Лечить все**.

### СМ. ТАКЖЕ

Изменение действия над обнаруженными объектами .....[42](#)

# ПРОВЕРКА СЕРВЕРА НА ВИРУСЫ

Антивирус Касперского 6.0 для Windows Servers MP4 позволяет проверять на присутствие вирусов как отдельные объекты (файлы, папки, диски, сменные устройства), так и весь сервер в целом. Проверка на вирусы позволяет исключить возможность распространения вредоносного кода, не обнаруженного Файловым Антивирусом по тем или иным причинам.

В состав Антивируса Касперского 6.0 для Windows Servers MP4 по умолчанию включены следующие задачи проверки на вирусы:

## Проверка

Проверка объектов, выбранных пользователем. Вы можете проверить любой объект файловой системы компьютера.

## Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски.

## Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

По умолчанию данные задачи выполняются с рекомендуемыми параметрами. Вы можете изменять эти параметры, а также устанавливать расписание запуска задач.

Кроме того, вы можете проверить на вирусы любой объект, не создавая для этого специальной задачи проверки. Выбрать объект для проверки можно из интерфейса Антивируса Касперского или стандартными средствами операционной системы Microsoft Windows Server (например, в окне программы **Проводник** или на **Рабочем столе** и т.д.). Для этого установите курсор мыши на имени выбранного объекта, правой клавишей мыши откройте контекстное меню Microsoft Windows и выберите пункт **Проверить на вирусы**.

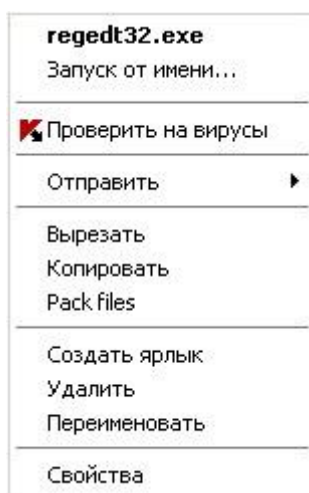


Рисунок 7. Контекстное меню Microsoft Windows

Также вы можете перейти к отчету о проверке, где будет представлена полная информация о событиях, произошедших в ходе выполнения задач.

➡ Чтобы изменить параметры какой-либо задачи проверки на вирусы, выполните следующие действия:

1. Откройте главное окно программы.

2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в настройки параметров для выбранной задачи внесите необходимые изменения.

➔ *Чтобы перейти к отчету о проверке на вирусы, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Нажмите на кнопку **Отчеты**.

## В ЭТОМ РАЗДЕЛЕ

---

Запуск проверки на вирусы.....	<a href="#">51</a>
Формирование списка объектов проверки.....	<a href="#">53</a>
Изменение уровня безопасности .....	<a href="#">53</a>
Изменение действия при обнаружении угрозы .....	<a href="#">54</a>
Изменение типа проверяемых объектов .....	<a href="#">55</a>
Оптимизация проверки.....	<a href="#">55</a>
Проверка составных файлов .....	<a href="#">56</a>
Изменение метода проверки .....	<a href="#">57</a>
Технология проверки.....	<a href="#">57</a>
Производительность компьютера при выполнении задач .....	<a href="#">58</a>
Приостановка задачи: формирование расписания .....	<a href="#">58</a>
Приостановка работы компонента: формирование списка программ .....	<a href="#">59</a>
Режим запуска: задание учетной записи .....	<a href="#">59</a>
Режим запуска: формирование расписания.....	<a href="#">59</a>
Особенности запуска задачи проверки по расписанию.....	<a href="#">60</a>
Статистика проверки на вирусы .....	<a href="#">60</a>
Назначение единых параметров проверки для всех задач.....	<a href="#">61</a>
Восстановление параметров проверки по умолчанию .....	<a href="#">61</a>

## ЗАПУСК ПРОВЕРКИ НА ВИРУСЫ

Запустить задачу проверки на вирусы можно двумя способами:

- из контекстного меню Антивируса Касперского;

- из главного окна Антивируса Касперского.

Информация о процессе выполнения задачи будет отображаться в главном окне Антивируса Касперского.

Кроме того, вы можете выбрать объект для проверки стандартными средствами операционной системы Microsoft Windows (например, в окне программы **Проводник** или на **Рабочем столе** и т. д.).

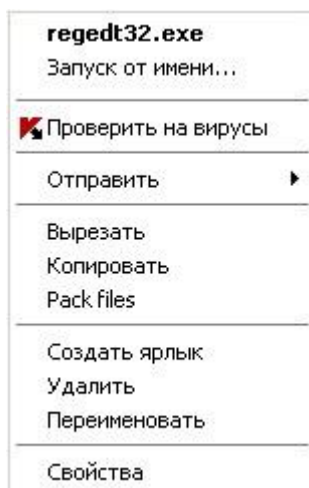


Рисунок 8. Контекстное меню Microsoft Windows

➤ Чтобы запустить задачу проверки на вирусы из контекстного меню, выполните следующие действия:

1. В области уведомлений панели задач нажмите правой клавишей мыши на значок программы.
2. В раскрывшемся меню выберите пункт **Проверка**. В открывшемся главном окне Антивируса Касперского выберите нужную задачу **Проверка (Полная проверка, Быстрая проверка)**. Произведите, если необходимо, настройку параметров выбранной задачи и нажмите на кнопку **Выполнить проверку**.
3. Либо в контекстном меню выберите пункт **Проверка Моего компьютера**. Будет запущена полная проверка компьютера. Процесс выполнения задачи будет отображаться в главном окне Антивируса Касперского.

➤ Чтобы запустить задачу проверки на вирусы из главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на кнопку **Выполнить проверку**. Процесс выполнения задачи будет отображаться в главном окне программы.

➤ Чтобы запустить задачу проверки на вирусы для выбранного объекта из контекстного меню Microsoft Windows, выполните следующие действия:

1. Нажмите правой клавишей мыши на имени выбранного объекта.
2. В раскрывшемся меню выберите пункт **Проверить на вирусы**. Прогресс и результат выполнения задачи будет отображаться в окне статистики.

## ФОРМИРОВАНИЕ СПИСКА ОБЪЕКТОВ ПРОВЕРКИ

По умолчанию каждой задаче проверки на вирусы соответствует свой список объектов. Чтобы просмотреть этот список, в разделе **Проверка** главного окна программ выберите имя задачи (например, **Полная проверка**). Список объектов будет представлен в правой части окна.

Для задач, созданных по умолчанию при установке программы, списки объектов для проверки уже сформированы.

Для удобства пользователей доступно добавление в область проверки таких категорий, как почтовые ящики пользователя, системная память, объекты автозапуска, резервное хранилище операционной системы, объекты, находящиеся в карантинном каталоге Антивируса Касперского.

Кроме того, при добавлении в область проверки каталога, содержащего вложенные объекты, вы можете изменять рекурсию. Для этого выберите объект в списке объектов проверки, откройте контекстное меню и воспользуйтесь командой **Включая вложенные папки**.

➔ *Чтобы сформировать список объектов для проверки, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку **Добавить**.
4. В открывшемся окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **Добавить**. После добавления всех нужных объектов нажмите на кнопку **ОК**. Чтобы исключить какие-либо объекты из проверки, снимите флажки рядом с ними в списке. Чтобы удалить объект из списка, выберите его и нажмите на ссылку **Удалить**.

## ИЗМЕНЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ

Под уровнем безопасности подразумевается предустановленный набор параметров проверки. Специалистами «Лаборатории Касперского» сформированы три уровня безопасности. Решение о том, какой уровень выбрать, вы принимаете самостоятельно на основе собственных предпочтений:

- если вы подозреваете, что вероятность заражения вашего компьютера очень высока, выберите высокий уровень безопасности.
- рекомендуемый уровень подходит для большинства случаев, и именно его рекомендуют использовать специалисты «Лаборатории Касперского».
- если вы работаете с программами, требующими значительных ресурсов оперативной памяти, выберите низкий уровень безопасности, поскольку набор проверяемых файлов на данном уровне сокращен.

Если ни один из предложенных уровней не отвечает вашим требованиям, вы можете настроить параметры работы проверки самостоятельно. В результате название уровня безопасности изменится на **Другой**. Чтобы восстановить параметры работы проверки по умолчанию, выберите один из предустановленных уровней. По умолчанию проверка осуществляется на **Рекомендуемом** уровне.

➔ *Чтобы изменить установленный уровень безопасности, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Уровень безопасности** переместите ползунок по шкале. Регулируя уровень безопасности, вы определяете соотношение между скоростью выполнения проверки и

количеством проверяемых файлов: чем меньше файлов анализируется на присутствие вирусов, тем выше скорость проверки. Либо нажмите на кнопку **Настройка** и в открывшемся окне настройте необходимые параметры. Уровень безопасности изменится на **Другой**.

## ИЗМЕНЕНИЕ ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ УГРОЗЫ

Если в результате проверки объекта на вирусы выясняется, что он заражен или подозреваем на заражение, дальнейшие операции программы зависят от статуса объекта и выбранного действия.

По результатам проверки объекту может быть присвоен один из следующих статусов:

- статус одной из вредоносных программ (например, *вирус, троянская программа*).
- *возможно зараженный*, когда в результате проверки однозначно невозможно определить, заражен объект или нет. Вероятно, в файле обнаружена последовательность кода неизвестного вируса или модифицированный код известного вируса.

По умолчанию все зараженные файлы подвергаются лечению, а все возможно зараженные – помещаются на карантин.

Если в качестве действия вы выбрали	При обнаружении вредоносного/ возможно зараженного объекта
<input checked="" type="radio"/> <b>Запросить по окончании проверки</b>	Программа откладывает обработку объектов до конца проверки. По окончании проверки на экран один за другим будут выводиться окна с запросом действия над каждым из объектов.
<input checked="" type="radio"/> <b>Запросить во время проверки</b>	Программа выводит на экран предупреждающее сообщение, содержащее информацию о том, каким вредоносным кодом заражен/ возможно заражен объект, и предлагает на выбор одно из дальнейших действий.
<input checked="" type="radio"/> <b>Не запрашивать</b>	Программа фиксирует информацию об обнаруженных объектах в отчете, не обрабатывая их и не уведомляя пользователя. Не рекомендуется устанавливать данный режим работы программы, поскольку зараженные и возможно зараженные объекты остаются на вашем компьютере и избежать заражения практически невозможно.
<input checked="" type="radio"/> <b>Не запрашивать</b> <input checked="" type="checkbox"/> <b>Лечить</b>	Программа фиксирует информацию об обнаруженных объектах в отчете, не обрабатывая их и не проводя уведомление. Не рекомендуется устанавливать данный режим работы программы, поскольку зараженные и возможно зараженные объекты остаются на сервере и избежать заражения практически невозможно.
<input checked="" type="radio"/> <b>Не запрашивать</b> <input checked="" type="checkbox"/> <b>Лечить</b> <input checked="" type="checkbox"/> <b>Удалить, если лечение невозможно</b>	Программа, не запрашивая подтверждения пользователя, выполняет попытку лечения обнаруженного объекта. Если попытка лечения объекта не удалась, он удаляется. Копия объекта сохраняется в резервном хранилище.
<input checked="" type="radio"/> <b>Не запрашивать</b> <input type="checkbox"/> <b>Лечить</b> <input checked="" type="checkbox"/> <b>Удалить</b>	Программа автоматически удаляет объект.

Перед лечением или удалением объекта Антивирус Касперского формирует его резервную копию и помещает ее в резервное хранилище на тот случай, если понадобится восстановить объект или появится возможность его вылечить.

При статусе *возможно зараженный* объект помещается на карантин без попытки лечения.

➤ *Чтобы изменить установленное действие над обнаруженными объектами, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Действие** внесите необходимые изменения.

## ИЗМЕНЕНИЕ ТИПА ПРОВЕРЯЕМЫХ ОБЪЕКТОВ

Указывая тип проверяемых объектов, вы определяете, файлы какого формата и размера будут проверяться при выполнении выбранной задачи проверки.

При выборе типа файлов следует помнить следующее:

- Для файлов некоторых форматов (например, *txt*) вероятность внедрения и последующей активации вредоносного кода достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, *exe*, *dll*, *doc*). Риск внедрения и активации в такие файлы вредоносного кода весьма высок.
- Не стоит забывать, что злоумышленник может отправить вирус на ваш компьютер в файле с расширением *txt*, тогда как на самом деле это будет исполняемый файл, переименованный в *txt*-файл. Если вы выберете вариант  **Файлы, проверяемые по расширению**, то в процессе проверки такой файл будет пропущен. Если же выбран вариант  **Файлы, проверяемые по формату**, невзирая на расширение, защита файлов проанализирует заголовки и выяснит, что файл имеет *exe*-формат. Такой файл будет подвергнут тщательной проверке на вирусы.

➤ *Чтобы изменить тип проверяемых файлов, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Типы файлов** выберите нужный параметр.

## ОПТИМИЗАЦИЯ ПРОВЕРКИ

Вы можете сократить время проверки и увеличить скорость работы Антивируса Касперского. Для этого следует проверять только новые файлы и те, что изменились с момента предыдущего их анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Кроме того, вы можете задать ограничение длительности проверки. По истечении заданного времени проверка файлов будет прекращена. Размер файла, подвергаемого проверке, также можно ограничить. Если он превысит установленное значение, файл будет исключен из проверки.

➤ *Чтобы проверять только новые и измененные файлы, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.

4. В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Оптимизация проверки** установите флажок  **Проверять только новые и измененные файлы**.

➤ *Чтобы задать временное ограничение на длительность проверки, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Оптимизация проверки** установите флажок  **Остановить проверку, если она длится более** и задайте длительность проверки одного файла в поле рядом.

➤ *Чтобы ограничить размер проверяемого файла, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** нажмите на кнопку **Дополнительно**.
6. В открывшемся окне **Составные файлы** установите флажок  **Не распаковывать составные файлы большого размера** и задайте размер файла в поле рядом.

## ПРОВЕРКА СОСТАВНЫХ ФАЙЛОВ

Распространенная практика сокрытия вирусов – внедрение их в составные файлы: архивы, базы данных, и т. д. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать, что может привести к значительному снижению скорости проверки.

Для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы или только новые. Для этого воспользуйтесь ссылкой рядом с названием объекта. Она меняет свое значение при щелчке по ней левой клавишей мыши. Если установлен режим проверки только новых и измененных файлов, выбор типа проверяемых составных файлов будет недоступен.

➤ *Чтобы изменить список проверяемых составных файлов, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** выберите нужный тип проверяемых составных файлов.



## ИЗМЕНЕНИЕ МЕТОДА ПРОВЕРКИ

В качестве метода проверки вы можете использовать *эвристический анализ*. Суть метода в анализе активности, которую объект производит в системе. Если активность типична для вредоносных объектов, то с достаточной долей вероятности объект будет признан вредоносным или подозрительным.

Дополнительно вы можете выбрать уровень детализации эвристического анализа, для этого передвиньте ползунок в одну из позиций: **поверхностный**, **средний** или **глубокий**.

Кроме этого метода проверки вы можете использовать поиск руткитов. *Руткит* (rootkit) – это набор утилит, обеспечивающих сокрытие вредоносных программ в операционной системе. Данные утилиты внедряются в систему, маскируя свое присутствие, а также наличие в системе процессов, папок, ключей реестра других вредоносных программ, описанных в конфигурации руткита. Если поиск включен, вы можете установить детальный уровень обнаружения руткитов (углубленный анализ). В этом случае будет выполняться тщательный поиск данных программ путем анализа большого количества объектов разного типа.

➔ *Чтобы использовать нужные методы проверки, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Методы проверки** выберите нужные методы проверки.

## ТЕХНОЛОГИЯ ПРОВЕРКИ

Дополнительно вы можете задать технологию, которая будет использоваться при проверке:

- **iChecker**. Технология позволяет увеличить скорость проверки за счет исключения некоторых объектов. Исключение объекта из проверки осуществляется по специальному алгоритму, учитывающему дату выпуска баз программы, дату предыдущей проверки объекта, а также изменение параметров проверки.

Например, у вас есть файл архива, который был проверен Антивирусом Касперского и получил статус *не заражен*. В следующий раз этот архив будет исключен из проверки, если он не был изменен и не менялись параметры проверки. Если вы изменили состав архива, добавив в него новый объект, изменили параметры проверки, обновили базы программы, архив будет проверен повторно.

Технология iChecker имеет ограничение: она не работает с файлами больших размеров и применима только к объектам с известной программе структурой (например, файлы exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift**. Технология является развитием технологии iChecker для компьютеров с файловой системой NTFS. Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе, а кроме того, применима только к объектам, расположенным в файловой системе NTFS.

➔ *Чтобы использовать технологию проверки объектов, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Дополнительно** в блоке **Технологии проверки** включите использование нужной технологии.

## ПРОИЗВОДИТЕЛЬНОСТЬ КОМПЬЮТЕРА ПРИ ВЫПОЛНЕНИИ ЗАДАЧ

В целях ограничения нагрузки на центральный процессор и дисковые подсистемы выполнение задач проверки на вирусы можно отложить.

Выполнение задач проверки увеличивает нагрузку на центральный процессор и дисковые подсистемы, тем самым замедляя работу других программ. По умолчанию при возникновении такой ситуации Антивирус Касперского приостанавливает выполнение задач проверки и высвобождает ресурсы системы для программ пользователя.

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Чтобы проверка не зависела от работы таких программ, не следует уступать им ресурсы системы.

Обратите внимание, что данный параметр можно настраивать индивидуально для каждой задачи проверки на вирусы. В этом случае настройка параметра, произведенная для конкретной задачи, имеет более высокий приоритет.

- *Чтобы отложить выполнение задач проверки на вирусы при замедлении работы других программ, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Методы проверки** установите флажок  **Уступать ресурсы другим программам**.

## ПРИОСТАНОВКА ЗАДАЧИ: ФОРМИРОВАНИЕ РАСПИСАНИЯ

При выполнении работ, требующих значительных ресурсов операционной системы, вы можете временно останавливать работу задачи проверки. Для того чтобы снизить нагрузку и обеспечить быстрый доступ к объектам, вы можете настроить отключение компонента в определенное время.

- *Чтобы настроить расписание приостановки задачи, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок **По расписанию** и нажмите на кнопку **Расписание**.

- В окне **Приостановка задачи** укажите время (в формате ЧЧ:ММ), в течение которого защита будет приостановлена (поля **Приостановить в** и **Возобновить в**).

## ПРИОСТАНОВКА РАБОТЫ КОМПОНЕНТА: ФОРМИРОВАНИЕ СПИСКА ПРОГРАММ

При выполнении работ, требующих значительных ресурсов операционной системы, вы можете временно останавливать работу задачи проверки. Для того чтобы снизить нагрузку и обеспечить быстрый доступ к объектам, вы можете настроить отключение компонента при работе с определенными программами.

- *Чтобы настроить приостановку задачи на время работы указанных программ, выполните следующие действия:*
  - Откройте главное окно программы.
  - В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
  - Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
  - В раскрывшемся меню выберите пункт **Настройка**.
  - В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок **При запуске программ** и нажмите на кнопку **Выбрать**.
  - В окне **Программы** сформируйте список программ, при работе которых работа компонента будет приостановлена.

## РЕЖИМ ЗАПУСКА: ЗАДАНИЕ УЧЕТНОЙ ЗАПИСИ

Вы можете задать учетную запись, с правами которой будет производиться проверка.

- *Чтобы запустить задачу с правами другой учетной записи, выполните следующие действия:*
  - Откройте главное окно программы.
  - В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
  - Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
  - В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
  - В открывшемся окне на закладке **Режим запуска** в блоке **Пользователь** установите флажок  **Запускать задачу с правами учетной записи**. В полях ниже задайте имя учетной записи и пароль.

## РЕЖИМ ЗАПУСКА: ФОРМИРОВАНИЕ РАСПИСАНИЯ

Все задачи проверки на вирусы можно запускать вручную или по сформированному расписанию.

По умолчанию для задач, созданных при установке программы, отключен автоматический запуск по расписанию. Исключение составляет задача быстрой проверки, которая выполняется каждый раз при включении компьютера.

При формировании расписания запуска задач необходимо определить интервал, с которым должна выполняться проверка.

Если по каким-либо причинам запуск невозможен (например, в заданное время компьютер был выключен), вы можете настроить автоматический запуск в тот момент, когда это станет возможным.

➤ *Чтобы настроить расписание запуска задачи проверки, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Режим запуска** нажмите на кнопку **Изменить**.
5. В открывшемся окне **Расписание** внесите необходимые изменения.

➤ *Чтобы настроить автоматический запуск пропущенной задачи, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Режим запуска** нажмите на кнопку **Изменить**.
5. В открывшемся окне **Расписание** в блоке **Настройка расписания** установите флажок  **Запускать пропущенную задачу**.

## ОСОБЕННОСТИ ЗАПУСКА ЗАДАЧИ ПРОВЕРКИ ПО РАСПИСАНИЮ

Все задачи проверки на вирусы можно запускать вручную или по сформированному расписанию.

Для задач, запускаемых по сформированному расписанию, вы можете использовать дополнительную возможность – *приостанавливать проверку по расписанию в том случае, если выключен скринсейвер или компьютер разблокирован*. Данная возможность позволяет отложить запуск задачи до того момента, когда пользователь закончит работу на компьютере. Таким образом, задача проверки не будет занимать ресурсы компьютера во время его работы.

➤ *Чтобы запускать проверку только после того, как пользователь закончит свою работу, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Полная проверка, Быстрая проверка**.
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Режим запуска** установите флажок  **Приостанавливать проверку по расписанию, если выключен скринсейвер или разблокирован компьютер**.

## СТАТИСТИКА ПРОВЕРКИ НА ВИРУСЫ

Общая информация о работе каждой задачи проверки на вирусы приводится в окне статистики. Здесь вы можете узнать, сколько объектов было проверено, сколько обнаружено вредоносных объектов и объектов, требующих обработки. Кроме того, здесь приведена информация о времени начала и окончания последнего выполнения задачи, а также о длительности проверки.

Основная информация о результатах проверки сгруппирована на следующих закладках:

- *Обнаружено* – содержит все опасные объекты, обнаруженные в процессе выполнения задачи;
- *События* – содержит полный список событий, возникших при выполнении задачи;
- *Статистика* – содержит статистические данные о проверенных объектах;
- *Параметры* – содержит параметры, в соответствии с которыми выполняется задача.

Если в результате выполнения задачи возникли какие-то ошибки, попробуйте запустить ее еще раз. Если попытка будет завершена с ошибкой, сохраните отчет с результатами выполнения задачи в файл по кнопке **Сохранить как**. Затем отправьте отчет в Службу технической поддержки. Специалисты «Лаборатории Касперского» обязательно помогут вам.

➤ *Чтобы просмотреть статистику выполнения задачи проверки на вирусы, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**, сформируйте задачу проверки и запустите ее на выполнение. Прогресс выполнения задачи будет отображаться в главном окне. Нажмите на ссылку **Подробнее**, чтобы перейти в окно статистики.

## НАЗНАЧЕНИЕ ЕДИНЫХ ПАРАМЕТРОВ ПРОВЕРКИ ДЛЯ ВСЕХ ЗАДАЧ

Каждая задача проверки выполняется в соответствии со своими параметрами. По умолчанию задачи, сформированные при установке программы на компьютер, выполняются с параметрами, которые рекомендованы экспертами «Лаборатории Касперского».

Вы можете настроить единые параметры проверки для всех задач. За основу будет взят набор параметров, используемых при проверке на вирусы отдельного объекта.

➤ *Чтобы назначить единые параметры проверки для всех задач, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Проверка**.
3. В правой части окна в блоке **Параметры других задач** нажмите на кнопку **Применить**. Подтвердите назначение единых параметров в окне запроса подтверждения.

## ВОССТАНОВЛЕНИЕ ПАРАМЕТРОВ ПРОВЕРКИ ПО УМОЛЧАНИЮ

Настраивая параметры выполнения задачи, вы всегда можете вернуться к рекомендуемым параметрам. Они считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

➤ *Чтобы восстановить параметры проверки объектов по умолчанию, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.

3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

# ОБНОВЛЕНИЕ ПРОГРАММЫ

Поддержка защиты в актуальном состоянии – залог безопасности. Каждый день в мире появляются новые вирусы, троянские и другие вредоносные программы, поэтому крайне важно быть уверенным в том, что ваша информация находится под надежной защитой.

Обновление программы загружает и устанавливает на сервер:

- **Базы программы**

Защита информации обеспечивается на основании баз программы. Файловый Антивирус использует их при поиске опасных объектов на сервере и их обезвреживании. Базы ежечасно пополняются записями о новых угрозах и способах борьбы с ними. Поэтому базы настоятельно рекомендуется регулярно обновлять.

- **Модули программы**

Помимо баз программы, можно обновлять и модули программы. Пакеты обновлений устраняют уязвимости Антивируса Касперского, добавляют новые функции или улучшают существующие.

Основным источником обновлений Антивируса Касперского являются специальные серверы обновлений «Лаборатории Касперского».

Для успешной загрузки обновлений с серверов необходимо, чтобы ваш компьютер был подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если параметры прокси-сервера не определяются автоматически, настройте параметры подключения к нему.

В процессе обновления модули программы базы на сервере сравниваются с расположенными в источнике обновлений. Если на сервере установлена последняя версия баз и модулей, на экран выводится информационное сообщение об актуальности защиты компьютера. Если базы и модули отличаются, на сервер будет установлена именно недостающая часть обновлений. Полное копирование баз и модулей не производится, что позволяет существенно увеличить скорость обновления и заметно снизить объем трафика.

Перед обновлением баз Антивирус Касперского создает их резервную копию, если по каким-либо причинам вы захотите вернуться к их использованию.

Возможность отката необходима, например, если вы обновили базы и в процессе работы они были повреждены. Вы сможете вернуться к предыдущему варианту баз, а позже попробовать обновить их еще раз.

Одновременно с обновлением программы вы можете выполнять копирование полученных обновлений в локальный источник. Данный сервис позволяет обновлять базы и модули программы на компьютерах сети в целях экономии интернет-трафика.

Вы также можете настроить режим автоматического запуска обновления.

В разделе **Обновление** отображается информация о текущем состоянии баз программы.

Вы можете перейти к отчету об обновлении, где будет представлена полная информация о событиях, произошедших в ходе выполнения задачи обновления. Также можно ознакомиться с обзором вирусной активности на сайте [www.kaspersky.ru](http://www.kaspersky.ru) (ссылка **Обзор вирусной активности**).

► *Чтобы изменить параметры какой-либо задачи обновления, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.

4. В открывшемся окне в настройки параметров для выбранной задачи внесите необходимые изменения.

➤ *Чтобы перейти к отчету об обновлении, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на кнопку **Отчеты**.

## В ЭТОМ РАЗДЕЛЕ

Запуск обновления .....	<a href="#">64</a>
Откат последнего обновления .....	<a href="#">65</a>
Выбор источника обновлений .....	<a href="#">65</a>
Региональные настройки .....	<a href="#">66</a>
Использование прокси-сервера .....	<a href="#">66</a>
Режим запуска: задание учетной записи .....	<a href="#">67</a>
Режим запуска: формирование расписания .....	<a href="#">67</a>
Выбор предмета обновления .....	<a href="#">68</a>
Изменение режима запуска задачи обновления .....	<a href="#">68</a>
Обновление из локальной папки .....	<a href="#">69</a>
Статистика обновления .....	<a href="#">70</a>
Возможные проблемы при обновлении .....	<a href="#">70</a>

## ЗАПУСК ОБНОВЛЕНИЯ

В любой момент вы можете запустить обновление программы. Оно будет производиться из выбранного вами источника обновлений.

Запустить обновление Антивируса Касперского можно двумя способами:

- из контекстного меню;
- из главного окна программы.

Информация о процессе обновления будет отображаться в главном окне программы.

Обратите внимание, что при выполнении обновления одновременно будет произведено копирование обновлений в локальный источник, при условии, что данный сервис включен.

➤ *Чтобы запустить обновление Антивируса Касперского из контекстного меню, выполните следующие действия:*

1. В области уведомлений панели задач нажмите правой клавишей мыши на значок программы.



2. В раскрывшемся меню выберите пункт **Обновление**.

➔ *Чтобы запустить обновление из главного окна Антивируса Касперского, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на кнопку **Выполнить обновление**. Процесс выполнения задачи будет отображаться в главном окне программы.

## ОТКАТ ПОСЛЕДНЕГО ОБНОВЛЕНИЯ

Каждый раз, когда вы запускаете обновление, Антивирус Касперского создает резервную копию используемых баз и модулей и только потом приступает к их обновлению. Это позволяет вам вернуться к использованию предыдущих баз после неудачного обновления.

Возможность отката полезна, например, в том случае, если часть баз была повреждена. Локальные базы могут быть повреждены либо самим пользователем, либо вредоносной программой, что возможно только в том случае, если самозащита программы отключена. Вы сможете вернуться к предыдущим базам, а позже попробовать обновить их еще раз.

➔ *Чтобы вернуться к использованию предыдущей версии баз, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку **Откат к предыдущим базам**.

## ВЫБОР ИСТОЧНИКА ОБНОВЛЕНИЙ

*Источник обновлений* – это ресурс, содержащий обновления баз и модулей программы Антивируса Касперского.

В качестве источника обновления вы можете использовать:

- *Сервер администрирования* – централизованное хранилище обновлений, расположенное на Сервере администрирования Kaspersky Administration Kit (подробнее смотрите Руководство администратора «Kaspersky Administration Kit»);
- *Серверы обновлений «Лаборатории Касперского»* – специальные интернет-сайты, на которые выкладываются обновления баз и модулей программы для всех продуктов «Лаборатории Касперского»;
- *HTTP- или FTP-серверы, локальные или сетевые каталоги* – локальный сервер или каталог, содержащий актуальный набор обновлений.

Если серверы обновлений «Лаборатории Касперского» вам недоступны (например, нет доступа к интернету), вы можете позвонить в наш центральный офис по телефонам +7 (495) 797-87-00, +7 (495) 645-79-39 и узнать адреса партнеров «Лаборатории Касперского», которые смогут предоставить вам обновления на дискетах или дисках в zip-формате.

Полученные на съемном диске обновления вы можете разместить как на некотором FTP- или HTTP-сайте, так и в локальном или сетевом каталоге.

При заказе обновлений на съемных дисках обязательно уточняйте, хотите ли вы получить обновления модулей программы.

Если в качестве источника обновлений выбран ресурс, расположенный вне локальной сети, для обновления необходимо соединение с интернетом.

Если в качестве источников обновлений выбрано несколько ресурсов, то в процессе обновления программа обращается к ним строго по списку и обновляется с первого доступного источника.

➤ Чтобы выбрать источник обновлений, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Источник обновлений** нажмите на кнопку **Добавить**.
6. В открывшемся окне **Выбор источника обновлений** выберите FTP-, HTTP-сайт или укажите его IP-адрес, символьное имя или URL-адрес.

## РЕГИОНАЛЬНЫЕ НАСТРОЙКИ

Если в качестве источника обновлений вы используете серверы обновлений «Лаборатории Касперского», можно выбрать предпочтительное для вас местоположение сервера для загрузки обновлений. Серверы «Лаборатория Касперского» расположены в нескольких странах мира. Выбор географически ближайшего к вам сервера обновления «Лаборатории Касперского» поможет сократить время и увеличить скорость получения обновлений.

➤ Чтобы выбрать ближайший сервер, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Источник обновлений** в блоке **Региональные параметры** выберите вариант  **Выбрать из списка** и в раскрывающемся списке выберите ближайшую к вашему текущему местоположению страну.

Если выбрать вариант  **Определять автоматически**, то при обновлении будет использоваться информация о текущем регионе из реестра операционной системы.

## ИСПОЛЬЗОВАНИЕ ПРОКСИ-СЕРВЕРА

Если для выхода в интернет используется прокси-сервер, необходимо настроить его параметры.

➤ Чтобы настроить параметры прокси-сервера, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Параметры прокси** настройте параметры прокси-сервера.

## РЕЖИМ ЗАПУСКА: ЗАДАНИЕ УЧЕТНОЙ ЗАПИСИ

В Антивирусе Касперского реализован сервис запуска обновления программы от имени другой учетной записи (имперсонация). По умолчанию данный сервис отключен, и задачи запускаются от имени текущей учетной записи, под которой вы зарегистрированы в системе.

Поскольку обновление программы может производиться из источника, к которому у вас нет доступа (например, к сетевому каталогу обновлений) или прав авторизованного пользователя прокси-сервера, вы можете воспользоваться данным сервисом, чтобы запускать обновление программы от имени пользователя, обладающего такими привилегиями.

Обратите внимание, что без использования запуска с правами обновление по расписанию будет выполняться с правами текущей учетной записи. В том случае, если на компьютере в данный момент не зарегистрирован ни один пользователь, не настроен запуск обновления с правами и выполняется обновление по расписанию, оно будет запущено с правами SYSTEM.

➤ *Чтобы запустить задачу с правами другой учетной записи, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Режим запуска** установите флажок  **Запускать задачу с правами учетной записи**. Ниже введите данные учетной записи, под которой будет запускаться задача: имя учетной записи и пароль.

## РЕЖИМ ЗАПУСКА: ФОРМИРОВАНИЕ РАСПИСАНИЯ

Все задачи проверки на вирусы можно запускать вручную или по сформированному расписанию.

При формировании расписания запуска задач необходимо определить интервал, с которым должно выполняться обновление.

Если по каким-либо причинам запуск задачи невозможен (например, в заданное время компьютер был выключен), вы можете настроить автоматический запуск, как только это станет возможным.

➤ *Чтобы настроить расписание запуска задачи проверки, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Режим запуска** нажмите на кнопку **Изменить**.
5. В открывшемся окне **Расписание** внесите необходимые изменения.

➤ *Чтобы настроить автоматический запуск пропущенной задачи, выполните следующие действия:*

1. Откройте главное окно программы.

2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Режим запуска** нажмите на кнопку **Изменить**.
5. В открывшемся окне **Расписание** в блоке **Настройка расписания** установите флажок  **Запускать пропущенную задачу**.

## ВЫБОР ПРЕДМЕТА ОБНОВЛЕНИЯ

Предмет обновления определяет, что именно будет обновляться:

- базы программы;
- модули программы.

Базы программы обновляются всегда, а модули программы – только в том случае, если установлен соответствующий режим.

Если на момент обновления в источнике присутствует пакет модулей программы, Антивирус Касперского получит и установит его после перезагрузки компьютера. До перезагрузки полученные обновления модулей установлены не будут.

Если следующее обновление программы происходит до перезагрузки компьютера и установки полученных ранее обновлений модулей программы, то будет произведено только обновление баз программы.

► *Чтобы в процессе обновления на ваш компьютер копировались и устанавливались обновления модулей программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** установите флажок  **Обновлять модули программы**.

## ИЗМЕНЕНИЕ РЕЖИМА ЗАПУСКА ЗАДАЧИ ОБНОВЛЕНИЯ

Режим запуска задачи обновления Антивируса Касперского вы выбираете в ходе работы мастера настройки программы (см. раздел «Настройка параметров обновления» на стр. [28](#)). Выбранный режим запуска можно изменить.

Запуск задачи обновления может производиться в одном из следующих режимов:

- **Автоматически**. Антивирус Касперского с заданной периодичностью проверяет наличие пакета обновлений в источнике обновления. При обнаружении свежих обновлений Антивирус Касперского скачивает их и устанавливает на компьютер. Такой режим обновления используется по умолчанию.

Антивирус Касперского будет производить попытку обновления через интервал, указанный в предыдущем пакете обновлений, что позволяет автоматически регулировать частоту обновлений в случае вирусных эпидемий и других опасных ситуаций. Программа будет своевременно получать самые последние обновления баз, сетевых атак и модулей программы, что исключит возможность проникновения опасных программ на ваш компьютер.

- **По расписанию** (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию.

- **Вручную.** В этом случае вы самостоятельно запускаете обновление программы. Антивирус Касперского обязательно уведомит вас о необходимости обновления.

➔ *Чтобы настроить режим запуска задачи обновления, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Режим запуска** выберите режим запуска задачи обновления. Если выбран режим обновления по расписанию сформируйте расписание.

## ОБНОВЛЕНИЕ ИЗ ЛОКАЛЬНОЙ ПАПКИ

Процедура получения обновлений из локальной папки организована следующим образом:

1. Один из компьютеров сети получает пакет обновлений Антивируса Касперского с веб-серверов «Лаборатории Касперского» в интернете либо из другого веб-ресурса, содержащего актуальный набор обновлений. Полученные обновления помещаются в папку общего доступа.
2. Другие компьютеры сети для получения обновлений программы обращаются к папке общего доступа.

Антивирус Касперского 6.0 получает с серверов «Лаборатории Касперского» только собственный пакет обновлений. Копирование обновлений для других программ «Лаборатории Касперского» рекомендуется выполнять через **Kaspersky Administration Kit**.

➔ *Чтобы включить режим копирования обновлений, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Распространение обновлений** установите флажок  **Копировать обновления в папку** и в поле ниже укажите путь к папке общего доступа, куда будут помещаться полученные обновления. Кроме того, путь можно выбрать в окне, открываемом по кнопке **Обзор**.

➔ *Чтобы обновление программы выполнялось из выбранной папки общего доступа, выполните на всех компьютерах сети следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Источник обновлений** нажмите на кнопку **Добавить**.
6. В открывшемся окне **Выбор источника обновлений** выберите папку или введите полный путь к ней в поле **Источник**.

7. На закладке **Источник обновлений** снимите флажок  **Серверы обновлений «Лаборатории Касперского»**.

## СТАТИСТИКА ОБНОВЛЕНИЯ

Общая информация о работе задач обновления приводится в окне статистики. Здесь вы можете узнать о событиях, возникших при выполнении задачи (закладка *События*) и просмотреть список параметров, в соответствии с которыми выполняется задача (закладка *Параметры*).

Если в результате выполнения задачи возникли какие-то ошибки, попробуйте запустить задачу еще раз. Если попытка завершится с ошибкой, сохраните отчет с результатами выполнения задачи в файл по кнопке **Сохранить как**. Затем отправьте отчет в Службу технической поддержки. Специалисты «Лаборатории Касперского» обязательно помогут вам.

Краткая статистика обновления приведена в верхней части окна статистики и содержит размер скопированных и установленных обновлений, скорость, с которой производилось обновление, длительность процедуры и другую информацию.

► *Чтобы просмотреть статистику выполнения задачи проверки на вирусы, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**, сформируйте задачу обновления и запустите ее на выполнение. Процесс выполнения задачи будет отображаться в главном окне. По ссылке [Подробно](#) можно перейти в окно статистики.

## ВОЗМОЖНЫЕ ПРОБЛЕМЫ ПРИ ОБНОВЛЕНИИ

В процессе обновления программных модулей Антивируса Касперского или сигнатур угроз могут возникнуть ошибки, связанные с неверной настройкой обновления, проблемами связи и т. д. В данном разделе справки мы постараемся рассмотреть большинство ошибок и дать советы, как их устранить. При возникновении ошибок, не описанных в справке, а также для получения детальных рекомендаций по их устранению попытайтесь найти информацию в Базе знаний на интернет-портале Службы технической поддержки в разделе «Если программа выдала ошибку...». Если рекомендации, представленные в данном разделе, не помогли решить проблему, или информация об ошибке отсутствует в Базе знаний, отправьте запрос в Службу технической поддержки.

<p><b>ОШИБКИ КОНФИГУРАЦИИ</b></p> <p>Ошибки данной группы возникают преимущественно из-за неправильной установки программы либо из-за изменения конфигурации программы, приводящей к ее неработоспособности.</p> <p><u>Общие рекомендации:</u></p> <p>При возникновении ошибок данной группы рекомендуется повторить попытку запуска обновления. При повторении ошибки в дальнейшем обратитесь в Службу технической поддержки.</p> <p>В случае, если проблема связана с неправильной установкой программы, рекомендуется переустановить ее.</p>
<p><i>Не указан ни один источник обновления</i></p> <p>Ни один из источников не содержит файлов для обновления. Возможно, в параметрах обновления не указан ни один источник обновления. Проверьте корректность настройки параметров обновления и повторите попытку.</p>
<p><i>Ошибка проверки лицензии</i></p> <p>Данная ошибка возникает в случае, если используемый программой файл ключа заблокирован и помещен в «черный» список лицензий.</p>
<p><i>Ошибка получения параметров обновления</i></p> <p>Внутренняя ошибка при получении параметров задачи обновления. Пожалуйста, проверьте корректность настройки параметров обновления и повторите попытку.</p>
<p><i>Недостаточно прав на обновление</i></p> <p>Данная ошибка обычно возникает при отсутствии прав доступа к источнику обновления или папке размещения обновлений у учетной записи, под которой обновление запускается. Рекомендуется проверить наличие прав у данной учетной записи.</p> <p>Подобная ошибка возникает также при попытке копирования файлов обновления в папку, которая не может быть создана.</p>
<p><i>Внутренняя ошибка</i></p> <p>Внутренняя ошибка логики работы задачи обновления. Пожалуйста, проверьте корректность параметров обновления и повторите попытку.</p>
<p><i>Ошибка проверки обновления</i></p> <p>Данная ошибка возникает в случае, если файлы, загруженные с источника обновления, не прошли внутреннюю проверку. Пожалуйста, повторите попытку обновления позже.</p>
<p><b>ОШИБКИ, ВОЗНИКАЮЩИЕ ПРИ РАБОТЕ С ПАПКАМИ И ФАЙЛАМИ</b></p> <p>Ошибки данной группы возникают при ограничении либо отсутствии у учетной записи, от имени которой запускается обновление, прав на доступ к источнику обновления или папке размещения обновлений.</p> <p><u>Общие рекомендации:</u></p> <p>При возникновении ошибок данной группы рекомендуется проверить наличие прав на доступ к указанным файлам и папкам у данной учетной записи.</p>
<p><i>Невозможно создать папку</i></p> <p>Данная ошибка возникает в случае, если невозможно создать папку в процессе выполнения процедуры обновления.</p>
<p><i>Недостаточно прав для выполнения файловой операции</i></p> <p>Данная ошибка возникает в случае, если учетная запись, от имени которой запущено обновление, не обладает необходимыми правами для выполнения операций с файлами.</p>
<p><i>Не найден файл или папка</i></p> <p>Данная ошибка возникает при отсутствии файла или папки, необходимых при обновлении. Рекомендуется проверить, что указанные файл, папка существуют и доступны.</p>

<p><i>Ошибка файловой операции</i></p> <p>Данная ошибка является внутренней ошибкой логики работы модуля обновления при выполнении операций с файлами.</p>
<p><b>СЕТЕВЫЕ ОШИБКИ</b></p> <p>Ошибки данной группы возникают при наличии проблем связи либо при некорректной настройке параметров подключения к сети.</p> <p><u>Общие рекомендации:</u></p> <p>При возникновении ошибок данной группы рекомендуется проверить подключение вашего компьютера к сети, корректность настройки параметров подключения, доступность источника обновления. После этого повторите попытку обновления. В случае неудачи обратитесь в Службу технической поддержки.</p>
<p><i>Сетевая ошибка</i></p> <p>В процессе получения файлов обновления произошла ошибка. При возникновении данной ошибки проверьте подключение вашего компьютера к сети.</p>
<p><i>Соединение разорвано</i></p> <p>Данная ошибка возникает в том случае, если по каким-либо причинам разорвано соединение с источником обновления.</p>
<p><i>Истекло время ожидания сетевой операции</i></p> <p>Превышено время ожидания соединения с источником обновления. При настройке параметров обновления программы вы могли установить строгий тайм-аут соединения с источником обновления. Если за данное время вашему компьютеру не удастся подключиться к серверу или каталогу обновлений, возникает такая ошибка. Рекомендуем в этом случае проверить правильность настроек сервиса обновления, а также доступность источника обновления.</p>
<p><i>Ошибка авторизации на FTP-сервере</i></p> <p>Данная ошибка возникает в случае, если неверно указаны параметры авторизации на FTP-сервере, который является источником обновления. Пожалуйста, убедитесь, что в параметрах FTP-сервера разрешена загрузка файлов для данной учетной записи.</p>
<p><i>Ошибка авторизации на прокси-сервере</i></p> <p>Данная ошибка возникает в случае, если при настройке параметров обновления через прокси-сервер неверно указаны имя и пароль, либо учетная запись, от имени которой запускается обновление, не обладает правами доступа к источнику обновления. Пожалуйста, отредактируйте параметры авторизации и повторите попытку обновления.</p>
<p><i>Ошибка разрешения DNS-имени</i></p> <p>Данная ошибка возникает в случае, если не обнаружен ни один источник обновления. Возможно, некорректно указан адрес источника обновления, неверны параметры соединения с сетью, либо недоступен DNS-сервер. Рекомендуется проверить параметры обновления, доступность источника обновления и повторить попытку.</p>
<p><i>Соединение с источником обновления не может быть установлено</i></p> <p>Данная ошибка возникает, если нет связи с источником обновления. Пожалуйста, проверьте корректность адреса источника обновления и повторите попытку.</p>
<p><i>Соединение с прокси-сервером не может быть установлено</i></p> <p>Данная ошибка возникает, если неверно указаны параметры подключения к прокси-серверу. Для решения проблемы рекомендуется проверить корректность данных параметров, доступность прокси-сервера, доступность сети и повторить попытку обновления.</p>
<p><i>Ошибка разрешения DNS-имени прокси-сервера</i></p> <p>Данная ошибка возникает в случае, если не обнаружен прокси-сервер. Рекомендуется проверить корректность параметров подключения к прокси-серверу и доступность DNS-сервера.</p>
<p><b>ОШИБКИ, СВЯЗАННЫЕ С ПОВРЕЖДЕНИЕМ БАЗ</b></p> <p>Ошибки данной группы связаны с наличием поврежденных файлов на источнике обновления.</p>



<p><u>Общие рекомендации:</u></p> <p>При выполнении обновления с веб-серверов «Лаборатории Касперского» повторите попытку запуска обновления. В случае неудачи обратитесь в Службу технической поддержки.</p> <p>При обновлении из другого источника (например, из локальной папки) рекомендуется обновить его содержимое с веб-серверов «Лаборатории Касперского». В случае повторения ошибки обратитесь в Службу технической поддержки.</p>
<p><i>Файл отсутствует на источнике обновления</i></p> <p>Все файлы, которые скачиваются и устанавливаются на ваш компьютер в процессе обновления, перечисляются в специальном файле, включенном в пакет. Данная ошибка возникает в том случае, если какой-либо файл присутствует в списке обновляемых, но отсутствует на источнике обновления.</p>
<p><i>Ошибка проверки подписи</i></p> <p>Данная ошибка может быть возвращена программой в случае, если электронная цифровая подпись загружаемого пакета обновлений повреждена либо не соответствует подписи «Лаборатории Касперского».</p>
<p><i>Индексный файл поврежден или отсутствует</i></p> <p>Данная ошибка возникает, если на источнике обновления отсутствует либо поврежден индексный файл в формате xml, согласно которому выполняется обновление.</p>
<p><b>ОШИБКИ, СВЯЗАННЫЕ С ОБНОВЛЕНИЕМ С СЕРВЕРА АДМИНИСТРИРОВАНИЯ KASPERSKY ADMINISTRATION KIT</b></p> <p>Ошибки данной группы связаны с наличием проблем обновления программы через Сервер администрирования Kaspersky Administration Kit.</p> <p><u>Общие рекомендации:</u></p> <p>В первую очередь убедитесь, что программа Kaspersky Administration Kit и ее компоненты (Сервер администрирования и Агент администрирования) установлены и запущены. Повторите попытку обновления. В случае неудачи перезапустите Агент администрирования и Сервер администрирования, повторите попытку обновления еще раз. Если решить проблему не удалось, обратитесь в Службу технической поддержки.</p>
<p><i>Ошибка соединения с Сервером администрирования</i></p> <p>Данная ошибка возникает, если подключение к Серверу администрирования Kaspersky Administration Kit невозможно. Рекомендуется проверить, что Агент администрирования установлен и запущен.</p>
<p><i>Ошибка регистрации в Агенте администрирования</i></p> <p>При возникновении данной ошибки следуйте общим рекомендациям по устранению ошибок данной группы. Если ошибка повторится, соберите подробный файл отчета (трассировку) обновления и Агента администрирования на этом компьютере и отправьте их в Службу технической поддержки через веб-форму, сопроводив описанием ситуации.</p>
<p><i>Невозможно установить соединение. Сервер администрирования перегружен и не может обслужить запрос</i></p> <p>В данном случае попытку обновления рекомендуется произвести позже.</p>
<p><i>Невозможно установить соединение с Сервером администрирования / Главным Сервером администрирования / Агентом администрирования, физическая ошибка / неизвестная ошибка</i></p> <p>При возникновении подобных ошибок рекомендуется повторить попытку обновления позже. В случае неудачи обратитесь в Службу технической поддержки.</p>
<p><i>Ошибка получения файла с Сервера администрирования, неверный аргумент для транспорта</i></p> <p>Если данная ошибка будет воспроизводиться в дальнейшем, обратитесь в Службу технической поддержки.</p>
<p><i>Ошибка получения файла с Сервера администрирования</i></p> <p>При возникновении подобных ошибок рекомендуется повторить попытку обновления позже. В случае неудачи обратитесь в Службу технической поддержки.</p>
<p><b>РАЗНЫЕ КОДЫ</b></p> <p>В данную группу включены ошибки, не относящиеся ни к одной из перечисленных выше групп.</p>
<p><i>Отсутствуют файлы для операции отката</i></p>

Данная ошибка возникает, если после выполненного отката обновлений произошла еще одна попытка отката, но между ними не было произведено обновление. Повторная операция отката будет невозможна до тех пор, пока не будет выполнено успешное обновление, в результате которого будет восстановлен резервный набор файлов.

# НАСТРОЙКА ПАРАМЕТРОВ ПРОГРАММЫ

Окно настройки параметров программы предназначено для быстрого доступа к основным настройкам Антивируса Касперского 6.0.

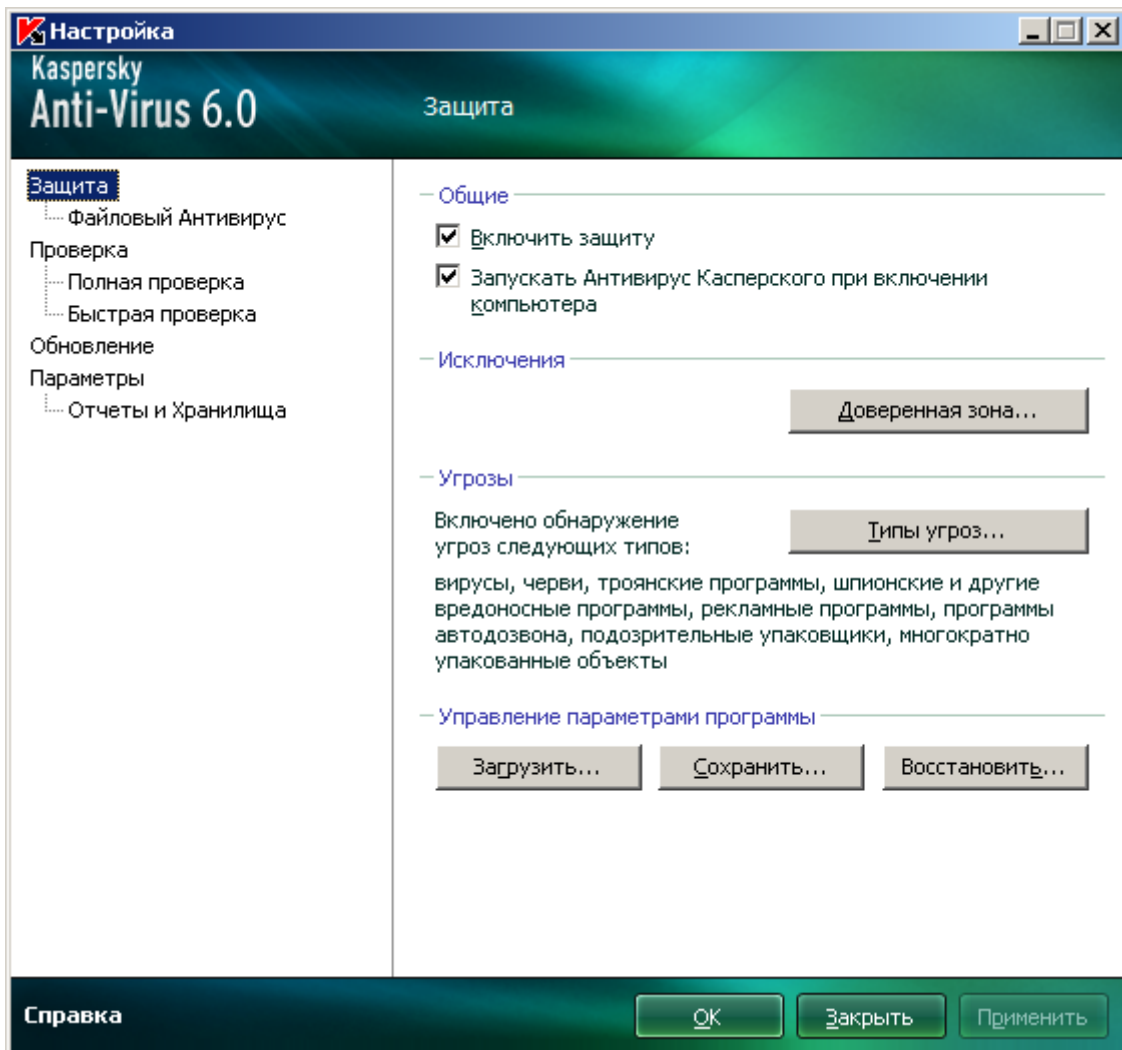


Рисунок 9. Окно настроек параметров приложения

Окно состоит из двух частей:

- левая часть окна обеспечивает доступ к Файлового Антивируса, задачам проверки на вирусы, обновления и др;
- правая часть окна содержит перечень параметров выбранного в левой части компонента, задачи и т. п.

Открыть окно можно следующими способами:

- Из главного окна программы. Для этого нажмите на кнопку **Настройка** в верхней части главного окна.

- Из контекстного меню. Для этого выберите пункт **Настройка** в контекстном меню программы.

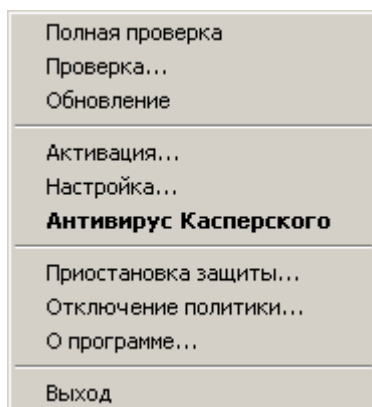


Рисунок 10. Контекстное меню

## В ЭТОМ РАЗДЕЛЕ

Защита.....	<a href="#">76</a>
Файловый Антивирус.....	<a href="#">83</a>
Проверка .....	<a href="#">83</a>
Обновление.....	<a href="#">84</a>
Параметры .....	<a href="#">85</a>
Отчеты и хранилища .....	<a href="#">90</a>

## ЗАЩИТА

В окне **Защита** вы можете воспользоваться следующими дополнительными функциями Антивируса Касперского:

- Отключение / включение защиты программы (см. стр. [77](#)).
- Запуск программы при старте операционной системы (см. стр. [77](#)).
- Выбор категорий обнаруживаемых угроз (см. стр. [77](#)).
- Формирование доверенной зоны (см. стр. [78](#)):
  - создание правила исключения (см. стр. [78](#));
  - формирование списка доверенных программ (см. стр. [81](#));
  - экспорт / импорт компонентов доверенной зоны (см. стр. [81](#)).
- Экспорт / импорт параметров работы программы (см. стр. [82](#)).
- Восстановление параметров работы программы по умолчанию (см. стр. [82](#)).

## ОТКЛЮЧЕНИЕ / ВКЛЮЧЕНИЕ ЗАЩИТЫ КОМПЬЮТЕРА

По умолчанию Антивирус Касперского запускается при старте операционной системы и защищает ваш компьютер в течение всего сеанса работы. Файловый Антивирус работает.

Вы можете отключить защиту, обеспечиваемую Файловым Антивирусом, полностью.

Специалисты «Лаборатории Касперского» настоятельно рекомендуют **не отключать защиту**, поскольку это может привести к заражению сервера и потере данных.

В результате отключения защиты работа Файлового Антивируса останавливается. Отключение работы компонента не оказывает влияния на выполнение задач проверки на вирусы и обновления Антивируса Касперского.

➔ Чтобы отключить защиту полностью, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. Снимите флажок  **Включить защиту**.

## ЗАПУСК ПРОГРАММЫ ПРИ СТАРТЕ ОПЕРАЦИОННОЙ СИСТЕМЫ

Если по какой-либо причине вам требуется полностью завершить работу Антивируса Касперского, выберите пункт **Выход** контекстного меню программы. В результате программа будет выгружена из оперативной памяти. Это подразумевает, что в данный период компьютер работает в незащищенном режиме.

Теперь включить защиту компьютера снова вы можете, загрузив программу из меню **Пуск** → **Программы** → **Антивирус Касперского 6.0** → **Антивирус Касперского 6.0**.

Кроме того, защита может быть запущена автоматически после перезагрузки операционной системы.

➔ Чтобы включить режим запуска программы при старте операционной системы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. Установите флажок  **Запускать Антивирус Касперского при включении компьютера**.

## ВЫБОР КАТЕГОРИЙ ОБНАРУЖИВАЕМЫХ УГРОЗ

Антивирус Касперского предлагает вам защиту от разных видов вредоносного программного обеспечения. Вне зависимости от установленных параметров, программа всегда проверяет и обезвреживает вирусы и троянские программы. Эти программы могут нанести значительный вред вашему компьютеру. Для обеспечения большей безопасности компьютера вы можете расширить список обнаруживаемых угроз, включив контроль потенциально опасных программ разного рода.

➔ Чтобы выбрать категории обнаруживаемых угроз, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Угрозы** нажмите на кнопку **Типы угроз**.

4. В открывшемся окне **Типы угроз** установите флажки  для тех категорий угроз, от которых вы хотите защитить свой компьютер.

## ФОРМИРОВАНИЕ ДОВЕРЕННОЙ ЗОНЫ

*Доверенная зона* – это сформированный пользователем перечень объектов, которые Антивирус Касперского не контролирует в процессе своей работы. Другими словами, это набор исключений из защиты программы.

Доверенную зону пользователь формирует самостоятельно, в зависимости от особенностей объектов, с которыми он работает, а также от того, какие программы установлены на его компьютере. Создание такого списка исключений может потребоваться, например, в случае, если Антивирус Касперского блокирует доступ к какому-либо объекту или программе, а вы уверены, что данный объект / программа абсолютно безвредны.

Исключать из проверки можно файл определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по классификации Вирусной энциклопедии (статусу, присвоенному объекту Антивирусом Касперского при проверке).

Объект исключения не подлежит проверке, если проверяется диск или папка, в которой он расположен. Однако при выборе проверки именно этого объекта правило исключения применено не будет.

➤ *Чтобы сформировать список исключений из защиты, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.
4. В открывшемся окне настройте правила исключений для объектов (см. стр. [78](#)), а также сформируйте список доверенных программ (см. стр. [81](#)).

### СМ. ТАКЖЕ

Создание правила исключения .....	<a href="#">78</a>
Разрешенные маски исключений файлов .....	<a href="#">79</a>
Разрешенные маски исключений по классификации Вирусной энциклопедии .....	<a href="#">80</a>
Формирование списка доверенных программ .....	<a href="#">81</a>
Экспорт / импорт компонентов доверенной зоны .....	<a href="#">81</a>

## СОЗДАНИЕ ПРАВИЛА ИСКЛЮЧЕНИЯ

*Правило исключения* – это совокупность условий, при которых объект не будет проверяться Антивирусом Касперского.

Исключать из проверки можно файл определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по классификации Вирусной энциклопедии.

*Тип угрозы* – это статус, который присвоен объекту Антивирусом Касперского при проверке. Статус присваивается на основании классификации вредоносных и потенциально-опасных программ, представленных в Вирусной энциклопедии «Лаборатории Касперского».

Потенциально опасное программное обеспечение не имеет какой-либо вредоносной функции, но может быть использовано в качестве вспомогательных компонентов вредоносной программы, поскольку содержит бреши и

ошибки. В эту категорию попадают, например, программы удаленного администрирования, IRC-клиенты, FTP-серверы, всевозможные утилиты для останова процессов или скрытия их работы, клавиатурные шпионы, программы вскрытия паролей, автоматического дозвона на платные сайты и т.д. Данное программное обеспечение не классифицируется как вирусы (not-a-virus), но его можно разделить на типы, например, Adware, Joke, Riskware и др. (подробную информацию о потенциально опасных программах, обнаруживаемых Антивирусом Касперского, смотрите в Вирусной энциклопедии на сайте [www.viruslist.ru](http://www.viruslist.ru) (<http://www.viruslist.com/ru/viruses/encyclopedia>)). В результате проверки такие программы могут быть заблокированы. Поскольку некоторые из них широко применяются пользователями, то предусмотрена возможность исключить их из проверки. Для этого нужно добавить в доверенную зону имя или маску угрозы по классификации Вирусной энциклопедии.

Например, вы часто используете в своей работе программу Remote Administrator. Это система удаленного доступа, позволяющая работать на удаленном компьютере. Такая активность программы рассматривается Антивирусом Касперского как потенциально опасная и может быть заблокирована. Чтобы исключить блокировку программы, нужно сформировать исключяющее правило, где в качестве классификации указать Remote Admin.

При добавлении исключения формируется правило, которое потом может использоваться Файловым Антивирусом, а также при выполнении задач проверки на вирусы

► *Чтобы создать правило исключения, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.
4. В открывшемся окне на закладке **Правила исключений** нажмите на кнопку **Добавить**.
5. В открывшемся окне **Правило исключения** в блоке **Параметры** выберите тип исключения. Затем в блоке **Описание** задайте значения для выбранных типов исключений и определите, в работе каких компонентов Антивируса Касперского должно быть использовано создаваемое правило.

► *Чтобы создать правило исключения из окна отчета, выполните следующие действия:*

1. В отчете выберите объект, который вы хотите добавить к исключениям.
2. В контекстном меню для этого объекта выберите пункт **Добавить в доверенную зону**.
3. В открывшемся окне **Правило исключения** убедитесь, что все параметры исключяющего правила вас устраивают. Поля с именем объекта и типом угрозы, который ему присвоен, заполняются автоматически на основании информации из отчета. Для создания правила нажмите на кнопку **ОК**.

## РАЗРЕШЕННЫЕ МАСКИ ИСКЛЮЧЕНИЙ ФАЙЛОВ

Рассмотрим примеры разрешенных масок, которые вы можете использовать при формировании списка исключаемых файлов:

1. Маски без путей к файлам:
  - **\*.exe** – все файлы с расширением exe;
  - **\*.ex?** – все файлы с расширением ex?, где вместо ? может использоваться любой один символ;
  - **test** – все файлы с именем test.
2. Маски с абсолютными путями к файлам:
  - **C:\dir\\*** или **C:\dir\\*** или **C:\dir\\*** – все файлы в папке C:\dir;
  - **C:\dir\\*.exe** – все файлы с расширением exe в папке C:\dir;

- **C:\dir\\*.ex?** – все файлы с расширением *ex?* в папке *C:\dir\*, где вместо *?* может использоваться любой символ;
- **C:\dir\test** – только файл *C:\dir\test*.

Чтобы не проверялись файлы во всех вложенных папках указанного каталога, при создании маски установите флажок  **Включая вложенные папки**.

3. Маски путей к файлам:

- **dir\\*.\*** или **dir\\*** или **dir\** – все файлы во всех папках *dir\*;
- **dir\test** – все файлы *test* в папках *dir\*;
- **dir\\*.exe** – все файлы с расширением *exe* во всех папках *dir\*;
- **dir\\*.ex?** – все файлы с расширением *ex?* во всех папках *dir\*, где вместо *?* может использоваться любой символ.

Чтобы не проверялись файлы во всех вложенных папках указанного каталога, при создании маски установите флажок  **Включая вложенные папки**.

Использовать маски исключения **\*.\*** или **\*** допустимо только при указании классификации исключаемой угрозы согласно Вирусной энциклопедии. В этом случае указанная угроза не будет обнаруживаться во всех объектах. Использование данных масок без указания классификации равносильно отключению защиты. Не рекомендуется также выбирать в качестве исключения путь, относящийся к виртуальному диску, сформированному на основе каталога файловой системы посредством команды *subst*, или к диску, который является отображением сетевой папки. Дело в том, что разные пользователи компьютера могут обозначать одним и тем же именем диска разные ресурсы, что неизбежно приведет к некорректному срабатыванию правил исключения.

**СМ. ТАКЖЕ**

Разрешенные маски исключений по классификации Вирусной энциклопедии .....[80](#)

**РАЗРЕШЕННЫЕ МАСКИ ИСКЛЮЧЕНИЙ ПО КЛАССИФИКАЦИИ ВИРУСНОЙ ЭНЦИКЛОПЕДИИ**

При добавлении в качестве исключения угрозы с определенным статусом по классификации Вирусной энциклопедии можно указать следующие данные:

- полное имя угрозы, как оно представлено в вирусной энциклопедии на сайте [www.viruslist.ru](http://www.viruslist.ru) (<http://www.viruslist.com/ru/viruses/encyclopedia>) (например, **not-a-virus:RiskWare.RemoteAdmin.RA.311** или **Flooder.Win32.Fuxx**);
- имя угрозы по маске, например:
  - **not-a-virus\*** – исключать из проверки легальные, но потенциально опасные программы, а также программы-шутки;
  - **\*Riskware.\*** – исключать из проверки все потенциально опасные программы типа Riskware;
  - **\*RemoteAdmin.\*** – исключать из проверки все версии программы удаленного администрирования.



**СМ. ТАКЖЕ**

Разрешенные маски исключений файлов ..... [79](#)

**ФОРМИРОВАНИЕ СПИСКА ДОВЕРЕННЫХ ПРОГРАММ**

Вы можете формировать список доверенных программ, активность которых, в том числе и подозрительная, а также файловая, сетевая активность и обращения к системному реестру не будут контролироваться.

Например, вы считаете объекты, используемые стандартной программой Microsoft Windows – **Блокнот**, безопасными и не требующими проверки. Другими словами, вы доверяете этой программе. Чтобы исключить проверку объектов, используемых данным процессом, добавьте программу **Блокнот** в список доверенных программ. Однако исполняемый файл и процесс доверенной программы по-прежнему будут проверяться на вирусы. Для полного исключения программы из проверки следует пользоваться правилами исключений.

Кроме того, некоторые действия, классифицирующиеся как опасные, являются нормальными в рамках функциональности ряда программ. Так, например, перехват текста, вводимого вами с клавиатуры, является нормальным действием для программ автоматического переключения раскладок клавиатуры (Punto Switcher и др.). Для того чтобы учесть специфику таких программ и отключить контроль их активности, мы рекомендуем добавить их в список доверенных.

Также использование исключения доверенных программ из проверки позволяет решать возможные проблемы совместимости Антивируса Касперского с другими программами (например, сетевой трафик с другого компьютера, уже проверенный антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

По умолчанию Антивирус Касперского проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и сетевой трафик, создаваемый ими.

➤ *Чтобы добавить программу в список доверенных, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.
4. В открывшемся окне на закладке **Доверенные программы** нажмите на кнопку **Добавить**.
5. В открывшемся окне **Доверенная программа** выберите программу воспользовавшись кнопкой **Обзор**. Будет открыто контекстное меню, в котором из пункта **Обзор** вы можете перейти в стандартное окно выбора файлов и указать путь к исполняемому файлу, или из пункта **Программы** перейти к списку программ, работающих в данный момент, и выбрать нужную. Для выбранной программы укажите нужные параметры.

**ЭКСПОРТ / ИМПОРТ КОМПОНЕНТОВ ДОВЕРЕННОЙ ЗОНЫ**

С помощью экспорта и импорта вы можете переносить сформированные правила исключений и списки доверенных программ на другие компьютеры.

➤ *Чтобы копировать сформированные правила исключений, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.

4. В открывшемся окне на закладке **Правила исключений** воспользуйтесь кнопками **Экспорт** и **Импорт**, чтобы выполнить необходимые действия по копированию правил.

➤ *Чтобы копировать сформированный список доверенных программ, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.
4. В открывшемся окне на закладке **Доверенные программы** воспользуйтесь кнопками **Экспорт** и **Импорт**, чтобы выполнить необходимые действия по копированию списка.

## ЭКСПОРТ / ИМПОРТ ПАРАМЕТРОВ РАБОТЫ АНТИВИРУСА КАСПЕРСКОГО

Антивирус Касперского предоставляет возможность экспортировать и импортировать свои параметры.

Это полезно, например, в том случае, когда программа установлена у вас на домашнем компьютере и в офисе. Дома вы можете настроить программу на удобный для себя режим работы, сохранить эти параметры на диск и с помощью функции импорта быстро загрузить их на свой рабочий компьютер. Параметры хранятся в специальном конфигурационном файле.

➤ *Чтобы экспортировать текущие параметры работы программы, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Управление параметрами программы** нажмите на кнопку **Сохранить**.
4. В открывшемся окне введите название конфигурационного файла и укажите место его сохранения.

➤ *Чтобы импортировать параметры работы из конфигурационного файла, выполните следующие действия*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Управление параметрами программы** нажмите на кнопку **Загрузить**.
4. В открывшемся окне выберите файл, из которого вы хотите импортировать параметры Антивируса Касперского.

## ВОССТАНОВЛЕНИЕ ПАРАМЕТРОВ ПО УМОЛЧАНИЮ

Вы всегда можете вернуться к рекомендуемым параметрам работы Антивируса Касперского. Они считаются оптимальными и рекомендованы специалистами «Лаборатории Касперского». Восстановление настроек осуществляется Мастером первоначальной настройки программы.

В открывшемся окне вам предлагается определить, какие параметры следует или не следует сохранять параллельно с восстановлением рекомендуемого уровня безопасности.

По завершении работы мастера для Файлового Антивируса будет установлен **Рекомендуемый** уровень безопасности с учетом тех параметров, которые вы решили сохранить при восстановлении. Кроме того, будут применены настройки, которые вы выполнили в ходе работы мастера.

➔ Чтобы восстановить параметры защиты, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Управление параметрами программы** нажмите на кнопку **Восстановить**.
4. В открывшемся окне установите флажки для тех параметров, для которых требуется сохранение. Нажмите на кнопку **Далее**. Будет запущен Мастер первоначальной настройки, следуйте его указаниям.

## ФАЙЛОВЫЙ АНТИВИРУС

В окне сгруппированы параметры для компонента **Файловый Антивирус** (см. раздел «Антивирусная защита файловой системы компьютера» на стр. [40](#)). Изменяя значения параметров, вы можете:

- изменять уровень безопасности (см. стр. [42](#));
- изменять действие над обнаруженными объектами (см. стр. [42](#));
- формировать область защиты (см. стр. [44](#));
- оптимизировать проверку (см. стр. [45](#));
- настраивать проверку составных файлов (см. стр. [45](#));
- изменять режим проверки (см. стр. [46](#));
- использовать эвристический анализ (см. стр. [45](#));
- приостанавливать работу компонента (см. стр. [47](#));
- выбирать технологию проверки (см. стр. [47](#));
- восстанавливать параметры защиты по умолчанию (см. стр. [48](#)), если они были изменены.

➔ Чтобы перейти к настройке параметров Файлового Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Файловый Антивирус**.
3. В правой части окна выберите уровень безопасности и реакцию на угрозу для компонента. Нажмите на кнопку **Настройка**, чтобы перейти к настройкам других параметров Файлового Антивируса.

## ПРОВЕРКА

То, каким образом осуществляется проверка объектов на вашем компьютере, определяется набором параметров, заданных для каждой задачи.

Специалистами ЗАО «Лаборатория Касперского» выделены несколько задач проверки на вирусы. В их число входят следующие:

### Проверка

Проверка объектов, выбранных пользователем. Вы можете проверить любой объект файловой системы компьютера.

## Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски.

## Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

В окне настройки для каждой из задач вы можете:

- выбрать уровень безопасности (см. стр. [53](#)), на основе параметров которого будет выполняться задача;
- выбрать действие (см. стр. [54](#)), которое будет применено программой при обнаружении зараженного / возможно зараженного объекта;
- сформировать расписание (см. стр. [59](#)) автоматического запуска задачи;
- определить типы файлов (см. стр. [55](#)), анализируемые на вирусы;
- определить параметры проверки составных файлов (см. стр. [56](#));
- выбрать методы и технологии проверки (см. стр. [57](#));
- назначить единые параметры проверки для всех задач (см. стр. [61](#)).

➔ *Чтобы перейти к настройке параметров задачи, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Проверка (Полная проверка, Быстрая проверка)**.
3. В правой части окна выберите нужный уровень безопасности, реакцию на угрозу и настройте режим запуска. Нажмите на кнопку **Настройка**, чтобы перейти к настройкам других параметров задач. Чтобы восстановить настройки параметров, принятые по умолчанию, нажмите на кнопку **По умолчанию**.

## ОБНОВЛЕНИЕ

Обновление Антивируса Касперского осуществляется в соответствии с параметрами, которые определяют:

- с какого ресурса (см. стр. [65](#)) производится копирование и установка обновлений программы;
- в каком режиме (см. стр. [68](#)) запускается процесс обновления программы, и что именно обновляется;
- как часто требуется запускать обновление, в случае если настроен запуск по расписанию (см. стр. [67](#));
- от имени какой учетной записи (см. стр. [67](#)) будет запущено обновление;
- требуется ли копировать полученные обновления в локальный источник (см. стр. [69](#));
- использование прокси-сервера (см. стр. [66](#)).

➔ *Чтобы перейти к настройке параметров обновления, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Обновление**.

3. В правой части окна выберите нужный режим запуска. Нажмите на кнопку **Настройка**, чтобы перейти к настройкам других параметров задачи.

## ПАРАМЕТРЫ

В окне **Параметры** вы можете воспользоваться следующими дополнительными функциями Антивируса Касперского:

- Самозащита программы (см. стр. [85](#)).
- Ограничение доступа к программе (см. стр. [86](#)).
- Ограничение размера iSwift-файлов (см. стр. [86](#)).
- Производительность работы сервера при использовании многопроцессорной конфигурации (см. стр. [87](#)).
- Уведомления о событиях Антивируса Касперского (см. стр. [87](#)):
  - выбор типа события и способа отправки уведомлений (см. стр. [88](#));
  - настройка отправки уведомлений по электронной почте (см. стр. [88](#));
  - настройка параметров журнала событий (см. стр. [89](#)).
- Активные элементы интерфейса (см. стр. [89](#)).

## САМОЗАЩИТА ПРОГРАММЫ

Антивирус Касперского обеспечивает безопасность компьютера от вредоносных программ, и в силу этого само становится объектом интереса со стороны вредоносного программного обеспечения, пытающегося заблокировать работу программы или даже удалить его с компьютера.

Чтобы обеспечить стабильность системы безопасности вашего компьютера, в программу добавлены механизмы самозащиты и защиты от удаленного воздействия.

В 64-разрядных операционных системах Microsoft Windows Server 2008 (без установленных Пакетов обновлений) и Microsoft Windows Server 2003 доступна только защита от изменений или удаления файлов программы на диске, а также записей в системном реестре.

При использовании защиты от удаленного воздействия возникает необходимость предоставить доступ к управлению программой программ удаленного администрирования (например, RemoteAdmin). Для этого следует добавить эти программы в список доверенных программ и включить для них параметр **Разрешать взаимодействие с интерфейсом программы**.

► *Чтобы включить использование механизмов самозащиты программы, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Самозащита** установите флажок  **Включить самозащиту**, чтобы задействовать механизм защиты программы от изменения или удаления собственных файлов на диске, процессов в памяти, записей в системном реестре.

В блоке **Самозащита** установите флажок  **Отключить возможность внешнего управления системной службой**, чтобы заблокировать любую попытку удаленного управления сервисами программы.

При попытке выполнить какое-либо из перечисленных действий над значком программы в области уведомлений панели задач Microsoft Windows будет открыто уведомление (если сервис уведомлений не отключен пользователем).

## ОГРАНИЧЕНИЕ ДОСТУПА К ПРОГРАММЕ

Персональный компьютер может использоваться несколькими людьми, в том числе с разным уровнем компьютерной грамотности. Открытый доступ к программе, ее параметрам может значительно снизить уровень безопасности компьютера в целом.

Чтобы повысить безопасность компьютера, используйте пароль для доступа к Антивирусу Касперского. Вы можете заблокировать все операции за исключением работы с уведомлениями об обнаружении опасных объектов; или запретить выполнение одного из следующих действий:

- изменение параметров работы программы;
- завершение работы программы;
- отключение работы Файлового Антивируса и задач проверки;
- отключение политики (при работе программы через Kaspersky Administration Kit);
- удаление программы.

Каждое из перечисленных выше действий приводит к снижению уровня защиты вашего компьютера, поэтому постарайтесь определить, кому из пользователей вашего компьютера вы доверяете выполнять такие действия.

► *Чтобы защитить доступ к программе с помощью пароля, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Защита паролем** установите флажок  **Включить защиту паролем** и нажмите на кнопку **Настройка**.
4. В открывшемся окне **Защита паролем** введите пароль и укажите область, на которую будет распространяться ограничение доступа. Теперь при попытке любого пользователя на вашем компьютере выполнить выбранные вами действия программа всегда будет запрашивать пароль.

## ОГРАНИЧЕНИЕ РАЗМЕРА iSWIFT-ФАЙЛОВ

*iSwift-файлы* – это файлы, содержащие информацию об уже проверенных на содержание вирусов объектах файловой системы NTFS (технология iSwift). Наличие таких файлов позволяет ускорить проверку объектов, поскольку Антивирус Касперского проверяет только те объекты, которые изменились со времени последней проверки. Со временем iSwift-файлы достигают большого размера. Рекомендуем вам установить ограничение размера таких файлов. При достижении заданного значения iSwift-файл будет очищен.

► *Чтобы ограничить размер iSwift-файлов, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Ресурсы** установите флажок  **Обнулять базу iSwift по достижении** и рядом укажите размер базы в мегабайтах.

## МНОГОПРОЦЕССОРНАЯ КОНФИГУРАЦИЯ СЕРВЕРА

При использовании многопроцессорной конфигурации сервера, вы можете настраивать производительность работы сервера, используя следующие приемы:

- Задавать число экземпляров антивирусного ядра, загружаемых при запуске Антивируса Касперского на сервере (то есть число параллельно запущенных на сервере антивирусных процессов).

Чем большее количество копий антивирусного ядра запущено, тем быстрее выполняется антивирусная обработка объектов. Однако это сказывается на общей производительности работы сервера. При недостаточном объеме оперативной памяти и большом количестве запущенных копий антивирусного ядра возможны сбои в работе Файлового Антивируса.

Кроме того, несколько одновременно запущенных антивирусных процессов позволяют обеспечить непрерывную защиту сервера в случае, например, сбоя в работе одного из ядер.

- Регулировать нагрузку на сервер: например, часть процессоров зарезервировать под антивирусную обработку объектов, а часть – под непосредственные задачи сервера.

Специалисты «Лаборатории Касперского» рекомендуют при работе на многопроцессорном сервере резервировать как минимум один процессор под задачи сервера.

➡ *Чтобы задать число экземпляров антивирусного ядра, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Производительность** нажмите на кнопку **Подробнее**.
4. В открывшемся окне **Многопроцессорная конфигурация** в блоке **Параметры** укажите количество копий антивирусного ядра.

➡ *Чтобы сбалансировать нагрузку на сервер, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Производительность** нажмите на кнопку **Подробнее**.
4. В открывшемся окне **Многопроцессорная конфигурация** в блоке **Используемые процессоры** снимите флажки  с тех процессоров, которые необходимо выделить непосредственно для работы сервера.

## УВЕДОМЛЕНИЯ О СОБЫТИЯХ АНТИВИРУСА КАСПЕРСКОГО

В процессе работы Антивируса Касперского возникают различного рода события. Они могут иметь информационный характер или нести важную информацию. Например, событие может уведомлять об успешно выполненном обновлении программы, а может фиксировать ошибку в работе некоторого компонента, которую необходимо срочно устранить.

Чтобы быть в курсе событий в работе Антивируса Касперского, воспользуйтесь сервисом уведомлений.

Уведомления могут быть реализованы одним из следующих способов:

- всплывающие сообщения над значком программы в системной панели;
- звуковое оповещение;
- сообщения электронной почты;

- запись информации в журнал событий.

► Чтобы воспользоваться сервисом уведомлений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Вид** установите флажок  **Включить уведомления о событиях** и нажмите на кнопку **Настройка**.
4. В открывшемся окне **Настройка уведомлений** определите типы событий Антивируса Касперского, о возникновении которых вы хотите быть уведомлены, а также способ уведомления.

## СМ. ТАКЖЕ

Выбор типа события и способа отправки уведомлений .....	<a href="#">88</a>
Настройка отправки уведомлений по электронной почте .....	<a href="#">88</a>
Настройка параметров журнала событий.....	<a href="#">89</a>

## ВЫБОР ТИПА СОБЫТИЯ И СПОСОБА ОТПРАВКИ УВЕДОМЛЕНИЙ

В процессе работы Антивируса Касперского возникают события следующих типов:

- **Критические события** – события критической важности, уведомления о которых настоятельно рекомендуется получать, поскольку они указывают на проблемы в работе программы или на уязвимости в защите вашего компьютера. Например, *базы сильно устарели* или *срок действия лицензии истек*.
- **Отказ функциональности** – события, приводящие к неработоспособности программы. Например, *базы отсутствуют или повреждены*.
- **Важные события** – события, на которые обязательно нужно обратить внимание, поскольку они отражают важные ситуации в работе программы. Например, *базы устарели* или *срок действия лицензии скоро закончится*.
- **Информационные события** – события справочного характера, как правило, не несущие важной информации. Например, *объект помещен на карантин*.

► Чтобы указать, о каких событиях и каким образом вы должны быть уведомлены, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Вид** установите флажок  **Включить уведомления о событиях** и нажмите на кнопку **Настройка**.
4. В открывшемся окне **Настройка уведомлений** установите флажки  для тех событий и тех способов отправки уведомлений, для которых хотите получать уведомления.

## НАСТРОЙКА ОТПРАВКИ УВЕДОМЛЕНИЙ ПО ЭЛЕКТРОННОЙ ПОЧТЕ

После того как выбраны события (см. раздел «Выбор типа события и способа отправки уведомлений» на стр. [88](#)), уведомления о возникновении которых вы хотите получать по электронной почте, следует настроить отправку уведомлений.



➤ Чтобы настроить отправку уведомлений по электронной почте, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Вид** установите флажок  **Включить уведомления о событиях** и нажмите на кнопку **Настройка**.
4. В открывшемся окне **Настройка уведомлений** установите флажки  для нужных событий в графе **Email** и нажмите на кнопку **Настройка email**.
5. В открывшемся окне **Настройка параметров почтовых уведомлений** задайте необходимые значения параметров. Для уведомления о событиях за определенный промежуток времени сформируйте расписание отправки информационного письма, нажав на кнопку **Изменить**. В открывшемся окне **Расписание** внесите необходимые изменения.

## НАСТРОЙКА ПАРАМЕТРОВ ЖУРНАЛА СОБЫТИЙ

Антивирус Касперского предоставляет возможность вносить информацию о событиях, возникающих в работе программы, в общий журнал событий Microsoft Windows (**Программа**) либо в отдельный журнал событий Антивируса Касперского (**Kaspersky Event Log**).

Просмотр журналов осуществляется в стандартном окне Microsoft Windows **Event Viewer**, которое можно вызвать с помощью команды **Пуск/Настройка/Панель управления/Администрирование/Просмотр событий**.

➤ Чтобы настроить параметры журнала событий, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Вид** установите флажок  **Включить уведомления о событиях** и нажмите на кнопку **Настройка**.
4. В открывшемся окне **Настройка уведомлений** установите флажки  для нужных событий в графе **Журнал** и нажмите на кнопку **Настройка журнала**.
5. В открывшемся окне **Параметры журнала событий** выберите журнал, в который будет записываться информация о событиях.

## АКТИВНЫЕ ЭЛЕМЕНТЫ ИНТЕРФЕЙСА

Под активными элементами интерфейса понимаются следующие возможности Антивируса Касперского:

**Анимировать значок в области уведомлений панели задач.**

В зависимости от выполняемой программой операции значок в системной панели меняется. Так, например, при проверке почтового сообщения на фоне значка появляется небольшая пиктограмма письма. По умолчанию анимация значка программы используется. В этом случае значок будет отражать только статус защиты вашего компьютера: если защита включена, значок – цветной, если защита приостановлена или выключена, значок становится серого цвета.

**Показывать «Protected by Kaspersky Lab» поверх экрана приветствия Microsoft Windows.**

По умолчанию такой индикатор появляется в правом верхнем углу экрана в момент запуска Антивируса Касперского. Он информирует вас о том, что защита вашего компьютера от любого рода угроз включена.

➤ Чтобы настроить активные элементы интерфейса, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Вид** установите нужные флажки.

## ОТЧЕТЫ И ХРАНИЛИЩА

В разделе собраны параметры, регулирующие работу с файлами данных программы.

*Файлы данных программы* – это объекты, помещенные в процессе работы Антивируса Касперского на карантин, в резервное хранилище, а также файлы отчета о работе компонентов программы.

В данном разделе вы можете:

- настроить параметры формирования и хранения отчетов;
- настроить параметры карантина и резервного хранилища;
- очистить содержимое хранилища отчетов, карантина и резервного хранилища.

➤ *Чтобы очистить содержимое хранилищ, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Отчеты и хранилища**.
3. В открывшемся окне нажмите на кнопку **Очистить**.
4. В открывшемся окне **Файлы данных** укажите, объекты каких хранилищ требуется удалить.

### СМ. ТАКЖЕ

Принципы работы с отчетами.....	<a href="#">90</a>
Карантин возможно зараженных объектов.....	<a href="#">91</a>
Действия с объектами на карантине.....	<a href="#">92</a>
Резервные копии опасных объектов.....	<a href="#">92</a>
Действия с резервными копиями.....	<a href="#">93</a>

## ПРИНЦИПЫ РАБОТЫ С ОТЧЕТАМИ

Работа Файлового Антивируса и выполнение каждой задачи проверки и обновления фиксируется в отчете.

➤ *Чтобы перейти к просмотру отчетов, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Отчеты**.

➤ *Чтобы ознакомиться со всеми событиями, зафиксированными в отчете о работе компонента или выполнении задачи, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Отчеты**.

2. В открывшемся окне на закладке **Отчеты** выберите имя компонента или задачи и нажмите на кнопку **Подробнее**. В результате будет открыто окно, содержащее детальную информацию о работе Файлового Антивируса или задачи. Результирующая статистика работы приведена в верхней части окна, а подробная информация размещена на разных закладках в центральной части. В зависимости от того, выбран отчет для Файлового Антивируса или задачи, состав закладок может быть разным.

➔ *Для того чтобы импортировать отчет в текстовый файл, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Отчеты**.
2. В открывшемся окне на закладке **Отчеты** выберите имя компонента или задачи и нажмите на кнопку **Подробнее**.
3. В открывшемся окне будет представлена информация о работе выбранного компонента или задачи. Нажмите на кнопку **Сохранить как** и укажите, куда бы вы хотели сохранить файл отчета.

## НАСТРОЙКА ПАРАМЕТРОВ ОТЧЕТОВ

Вы можете настроить следующие параметры формирования и хранения отчетов:

- Разрешить или запретить запись в отчет событий информационного характера. Как правило, такие события не принципиально важны для обеспечения защиты (флажок  **Записывать некритические события**).
- Включить хранение в отчете только событий, произошедших при последнем запуске задачи. Это позволит сэкономить место на диске за счет уменьшения размера отчета (флажок  **Хранить только текущие события**). Если флажок установлен, информация, представленная в отчете, будет обновляться при каждом перезапуске задачи. Однако перезаписи подлежит только информация некритического характера.
- Установить срок хранения отчетов (флажок  **Хранить отчеты не более**). По умолчанию срок хранения отчетов составляет 30 дней, после чего отчеты удаляются. Вы можете изменить максимальный срок хранения или совсем отменить это ограничение.
- Указать максимальный размер отчета (флажок  **Максимальный размер**). По умолчанию максимальный размер составляет 250 МБ. Вы можете отменить ограничение размера отчета или установить другое значение.

➔ *Чтобы настроить параметры формирования и хранения отчетов, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Отчеты и хранилища**.
3. В блоке **Отчеты** установите необходимые флажки и, если потребуется, установите срок хранения отчетов и укажите максимальный размер отчета.

## КАРАНТИН ВОЗМОЖНО ЗАРАЖЕННЫХ ОБЪЕКТОВ

**Карантин** – это специальное хранилище, в которое помещаются объекты, возможно зараженные вирусами.

**Возможно зараженные объекты** – это объекты, подозреваемые на заражение вирусами или их модификациями.

Почему *возможно зараженные*? Не всегда можно однозначно определить, является объект зараженным или нет. Причины могут быть следующие:

- *Код анализируемого объекта похож на известную угрозу, но частично изменен.*

Базы программы содержат те угрозы, которые на настоящее время изучены специалистами «Лаборатории Касперского». Если вредоносная программа изменяется и в базы эти изменения еще не внесены, то Антивирус Касперского отнесет объект, пораженный измененной вредоносной программой, к возможно зараженным объектам и обязательно укажет, на какую угрозу похоже это заражение.

- *Код обнаруженного объекта напоминает по структуре вредоносную программу, однако в базах программы ничего подобного не зафиксировано.*

Вполне возможно, что это новый вид угроз, поэтому Антивирус Касперского относит такой объект к возможно зараженным объектам.

Подозрение файла на присутствие в нем вируса определяется *эвристическим анализатором кода*. Этот механизм достаточно эффективен и очень редко приводит к ложным срабатываниям.

Возможно зараженный объект может быть обнаружен и помещен на карантин в процессе проверки на вирусы, а также Файловым Антивирусом.

При помещении объекта на карантин выполняется его перемещение, а не копирование: объект удаляется с диска или из почтового сообщения и сохраняется в карантинном каталоге. Файлы на карантине хранятся в специальном формате и не представляют опасности.

## СМ. ТАКЖЕ

Действия с объектами на карантине ..... [92](#)

## ДЕЙСТВИЯ С ОБЪЕКТАМИ НА КАРАНТИНЕ

С объектами, помещенными на карантин, вы можете производить следующие действия:

- помещать на карантин файлы, подозреваемые вами на присутствие вируса;
- проверять и лечить с использованием текущей версии баз программы все возможно зараженные объекты карантина;
- восстанавливать файлы в каталог, заданный пользователем, или каталоги, откуда они были перенесены на карантин (по умолчанию);
- удалять любой объект карантина или группу выбранных объектов.

➡ *Чтобы произвести какие-либо действия над объектами карантина, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Обнаружено**.
2. В открывшемся окне на закладке **Карантин** выполните необходимые действия.

## РЕЗЕРВНЫЕ КОПИИ ОПАСНЫХ ОБЪЕКТОВ

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

**Резервная копия** – копия оригинального опасного объекта, которая создается при первом лечении или удалении данного объекта и хранится в резервном хранилище.

**Резервное хранилище** – это специальное хранилище, содержащее резервные копии опасных объектов, подвергнутых обработке или удалению. Основная функция резервного хранилища – обеспечить возможность в любой момент восстановить исходный объект. Файлы в резервном хранилище хранятся в специальном формате и не представляют опасности.

**СМ. ТАКЖЕ**

Действия с резервными копиями..... [93](#)

**ДЕЙСТВИЯ С РЕЗЕРВНЫМИ КОПИЯМИ**

С объектами, находящимися в резервном хранилище, вы можете производить следующие действия:

- восстанавливать выбранные копии;
- удалять объекты.

➔ *Чтобы произвести какие-либо действия над объектами резервного хранилища, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Обнаружено**.
2. В открывшемся окне на закладке **Резервное хранилище** выполните необходимые действия.

**НАСТРОЙКА ПАРАМЕТРОВ КАРАНТИНА И РЕЗЕРВНОГО ХРАНИЛИЩА**

Вы можете настроить следующие параметры работы карантина и резервного хранилища:

- Задать режим автоматической проверки объектов на карантине после каждого обновления баз программы (флажок  **Проверять файлы на карантине после обновления**).

Антивирус Касперского не сможет проверить объекты карантина сразу после обновления баз программы, если в этот момент вы будете работать с карантином.

- Определить максимальный срок хранения объектов на карантине и копий объектов в резервном хранилище (флажок  **Хранить объекты не более**). По умолчанию срок хранения объектов составляет 90 дней, после чего объекты удаляются. Вы можете изменить максимальный срок хранения или совсем отменить это ограничение.
- Указать максимальный размер хранилища данных (флажок  **Максимальный размер**). По умолчанию максимальный размер составляет 1000 МБ. Вы можете отменить ограничение размера отчета или установить для него другое значение.

➔ Чтобы настроить параметры карантина и резервного хранилища, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Отчеты и хранилища**.
3. В блоке **Карантин и Резервное хранилище** установите необходимые флажки и, если потребуется, установите максимальный размер хранилища данных.

**ДИСК АВАРИЙНОГО ВОССТАНОВЛЕНИЯ**

В Антивирусе Касперского реализован сервис создания диска аварийного восстановления.

Диск аварийного восстановления предназначен для проверки и лечения зараженных x86-совместимых компьютеров. Он применяется при такой степени заражения, когда невозможно вылечить компьютер с помощью антивирусных программ или утилит лечения (например, Kaspersky AVPTool), запускаемых под управлением операционной системы. При этом эффективность лечения повышается за счет того, что находящиеся в системе вредоносные программы не получают управления во время загрузки операционной системы.

Диск аварийного восстановления формируется на базе ядра операционной системы Linux и представляет собой файл .iso, который включает:

- системные и конфигурационные файлы Linux;
- набор утилит для диагностики операционной системы;
- набор вспомогательных утилит (файловый менеджер и др.);
- файлы Kaspersky Rescue Disk;
- файлы, содержащие базы программы.

Загрузка компьютера с поврежденной операционной системой может осуществляться двумя способами:

- *локально*, с CD/DVD-ROM-устройства. Для этого на компьютере должно быть установлено соответствующее устройство.
- *удаленно*, с рабочего места администратора или другого компьютера сети.

Удаленная загрузка возможна только в случае, если загружаемый компьютер поддерживает технологию Intel® vPro™ или Intel® Active Management.

➔ Чтобы создать диск аварийного восстановления, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Диск аварийного восстановления** для запуска мастера создания диска (см. стр. [94](#)).
3. Следуйте указаниям мастера.
4. С помощью полученного в результате работы мастера файла создайте загрузочный CD/DVD-диск. Для этого можно воспользоваться одной из программ записи CD/DVD-дисков, например, Nero.

## СМ. ТАКЖЕ

Создание диска аварийного восстановления.....[94](#)

Загрузка компьютера с помощью диска аварийного восстановления.....[96](#)

## СОЗДАНИЕ ДИСКА АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

Создание диска аварийного восстановления заключается в формировании образа диска (файла .iso) с актуальными базами программы и конфигурационными файлами.

Исходный образ диска, на основе которого формируется новый файл, может быть загружен с сервера «Лаборатории Касперского» или скопирован с локального источника.

Сформированный мастером файл образа сохраняется в папке «Documents and Settings\All Users\Application Data\Kaspersky Lab\VP80\Data\Rdisk» («ProgramData\Kaspersky Lab\VP80\Data\Rdisk» – для Microsoft Vista) с именем *rescuecd.iso*. Если мастер обнаружил ранее созданный файл образа в указанной папке, то установив флажок  **Использовать существующий образ**, вы можете использовать его в качестве исходного образа

диска и перейти сразу к шагу 3 – обновление образа (см. стр. [95](#)). Если мастер не обнаружил файл образа, то данный флажок будет отсутствовать.

Диск аварийного восстановления создается с помощью мастера, который состоит из последовательности окон (шагов). Переключение между окнами осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

## РАССМОТРИМ ПОДРОБНЕЕ ШАГИ МАСТЕРА

Шаг 1. Выбор источника образа диска .....	<a href="#">95</a>
Шаг 2. Копирование (загрузка) образа диска.....	<a href="#">95</a>
Шаг 3. Обновление файла образа .....	<a href="#">95</a>
Шаг 4. Загрузка удаленного компьютера .....	<a href="#">96</a>
Шаг 5. Завершение работы мастера .....	<a href="#">96</a>

## ШАГ 1. ВЫБОР ИСТОЧНИКА ОБРАЗА ДИСКА

Если в предыдущем окне мастера вы установили  **Использовать существующий образ**, то этот шаг будет пропущен.

На данном этапе вам следует выбрать источник файла образа из предложенных вариантов:

- Выберите вариант  **Копировать образ с CD/DVD-диска или из локальной сети**, если у вас уже есть записанный CD/DVD-диск аварийного восстановления или подготовленный для него образ, сохраненный на вашем компьютере или на ресурсе локальной сети.
- Выберите вариант  **Загрузить образ с сервера «Лаборатории Касперского»**, если у вас нет сформированного файла образа, то вы можете загрузить его с сервера «Лаборатории Касперского» (размер файла составляет примерно 100 МБ).

## ШАГ 2. КОПИРОВАНИЕ (ЗАГРУЗКА) ОБРАЗА ДИСКА

Если на предыдущем шаге вы выбрали вариант копирования образа из локального источника ( **Копировать образ с CD/DVD-диска или из локальной сети**), то на данном шаге вам следует указать к нему путь. Для этого воспользуйтесь кнопкой **Обзор**. Далее будет отображен процесс копирования файла.

Если же вы выбрали вариант  **Загрузить образ с сервера «Лаборатории Касперского»**, то процесс загрузки файла отображается сразу.

## ШАГ 3. ОБНОВЛЕНИЕ ФАЙЛА ОБРАЗА

Процедура обновления файла образа включает:

- обновление баз программы;
- обновление конфигурационных файлов.

Конфигурационные файлы определяют способ применения диска аварийного восстановления: на локальном или удаленном компьютере, поэтому перед обновлением файла образа вам следует выбрать нужный вариант из предложенных:

- **Загрузка удаленного компьютера**, если предполагается загрузка удаленного компьютера.

Обратите внимание, что в случае загрузки удаленного компьютера, он должен поддерживать технологию Intel® vPro™ или Intel® Active Management.

Если доступ в интернет с удаленного компьютера осуществляется через прокси-сервер, то обновление при использовании диска аварийного восстановления будет недоступно. В этом случае рекомендуется предварительно выполнить обновление Антивируса Касперского.

- **Загрузка системы с CD/DVD-диска**, если создаваемый образ диска в дальнейшем будет записан на CD/DVD-диск.

Выбрав нужный вариант, нажмите на кнопку **Далее**. В следующем окне мастера будет отображен ход выполнения обновления.

Если выбран вариант **Загрузка удаленного компьютера**, то созданный образ не может быть использован для записи CD/DVD-диска и последующей загрузки компьютера. Для загрузки компьютера с CD/DVD-диска, необходимо запустить мастер заново и на этом шаге выбрать **Загрузка системы с CD/DVD-диска**.

## ШАГ 4. ЗАГРУЗКА УДАЛЕННОГО КОМПЬЮТЕРА

Данный шаг мастера появляется только в случае, если на предыдущем шаге вы выбрали вариант  **Загрузка удаленного компьютера**.

Укажите данные о компьютере:

- **IP-адрес или имя компьютера** в сети;
- данные учетной записи с правами администратора: **Имя пользователя** и **Пароль**.

Следующее окно мастера представляет собой консоль iAMT, где вы управляете процессом загрузки компьютера (см. стр. [96](#)).

## ШАГ 5. ЗАВЕРШЕНИЕ РАБОТЫ МАСТЕРА

В данном окне мастер проинформирует вас об успешном создании диска аварийного восстановления.

## ЗАГРУЗКА КОМПЬЮТЕРА С ПОМОЩЬЮ ДИСКА АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

Если в результате вирусной атаки невозможно загрузить операционную систему, воспользуйтесь диском аварийного восстановления.

Для загрузки операционной системы необходим файл образа (.iso) загрузочного диска. Вы можете загрузить (см. стр. [95](#)) файл с сервера «Лаборатории Касперского» или обновить (см. стр. [95](#)) существующий.

Рассмотрим подробнее работу диска аварийного восстановления. В процессе загрузки диска проводятся следующие операции:

1. Автоматическое определение аппаратного обеспечения компьютера.
2. Поиск файловых систем на жестких дисках. Найденным файловым системам назначаются имена начиная с C.



Имена, назначаемые жестким дискам и съемным устройствам, могут не совпадать с их наименованиями в операционной системе.

Если операционная система загружаемого компьютера находится в спящем режиме, или файловая система приведена в состояние *unclean* вследствие некорректного завершения работы, вам будет предложено принять решение о монтировании файловой системы или перезагрузке компьютера.

Монтирование файловой системы может привести к ее повреждению.

3. Поиск файла подкачки Microsoft Windows *pagefile.sys*. В случае его отсутствия размер виртуальной памяти ограничивается размером оперативной памяти.
4. Выбор языка локализации. Если в течение некоторого времени выбор не был сделан, то по умолчанию выбирается английский язык.

При загрузке удаленного компьютера данный шаг отсутствует.

5. Поиск (создание) папок для размещения антивирусных баз, отчетов, карантина и вспомогательных файлов. По умолчанию используются папки программы «Лаборатории Касперского», установленного на зараженном компьютере (*ProgramData/Kaspersky Lab/AVP8* – для Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8* – для более ранних версий Microsoft Windows). Если папки программы не найдены, будет произведена попытка создать их. В случае, если папки не были обнаружены и создать их не удалось, на одном из дисков создается папка *kl.files*.
6. Попытка настройки сетевых соединений на основе данных, обнаруженных в системных файлах загружаемого компьютера.
7. Загрузка графической подсистемы и запуск Kaspersky Rescue Disk (в случае загрузки компьютера с CD/DVD-диска).

В случае загрузки удаленного компьютера в консоли iAMT загружается командная строка. Для управления задачами используются команды для работы с Kaspersky Rescue Disk из командной строки (см. стр. [99](#)).


В режиме аварийного восстановления доступны только задачи проверки на вирусы и обновления баз с локального источника, а также откат обновлений и просмотр статистики.

➤ Чтобы произвести загрузку операционной системы зараженного компьютера с CD/DVD-ROM-диска, выполните следующие действия:

1. В параметрах BIOS включите загрузку с CD/DVD-ROM (подробную информацию можно получить из документации к материнской плате вашего компьютера).
2. Поместите в дисковод зараженного компьютера диск с предварительно записанным образом диска аварийного восстановления.
3. Перезагрузите компьютер.
4. Далее загрузка происходит в соответствии с описанным выше алгоритмом.

➤ Чтобы произвести загрузку операционной системы удаленного компьютера, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Диск аварийного восстановления** для запуска мастера создания диска (см. стр. [94](#)). Следуйте указаниям мастера.

Обратите внимание, что на этапе обновления (см. стр. [95](#)) образа диска вам необходимо выбрать вариант  **Загрузка удаленного компьютера**.

Далее загрузка происходит в соответствии с описанным выше алгоритмом.



# РАБОТА С KASPERSKY RESCUE DISK ИЗ КОМАНДНОЙ СТРОКИ

Работать с Kaspersky Rescue Disk можно посредством командной строки. При этом предусмотрена возможность выполнения следующих операций:

- проверка выбранных объектов;
- обновление баз и программных модулей;
- откат последнего обновления
- вызов справки по синтаксису командной строки;
- вызов справки по синтаксису команды.

Синтаксис командной строки:

<команда> [параметры]

В качестве команд используются:

<b>HELP</b>	помощь по синтаксису команды, вывод списка команд
<b>SCAN</b>	проверка объектов на присутствие вирусов
<b>UPDATE</b>	запуск задачи обновления
<b>ROLLBACK</b>	откат последнего произведенного обновления
<b>EXIT</b>	завершение работы с Kaspersky Rescue Disk

## **В ЭТОМ РАЗДЕЛЕ**

Проверка на вирусы .....	<a href="#">100</a>
Обновление Антивируса Касперского .....	<a href="#">101</a>
Откат последнего обновления .....	<a href="#">102</a>
Просмотр справки .....	<a href="#">102</a>

## ПРОВЕРКА НА ВИРУСЫ

Командная строка запуска проверки некоторой области на присутствие вирусов и обработки вредоносных объектов имеет следующий общий вид:

```
SCAN [<объект проверки>] [<действие>] [<типы файлов>] [<исключения>] [<параметры отчета>]
```

### Описание параметров:

<p><b>&lt;объект проверки&gt;</b> – параметр задает перечень объектов, которые будут проверены на присутствие вредоносного кода.</p> <p>Параметр может включать несколько значений из представленного списка, разделенных пробелом.</p>	
<b>&lt;files&gt;</b>	<p>Список путей к файлам и / или каталогам для проверки.</p> <p>Допускается ввод абсолютного или относительного пути. Разделительный символ для элементов списка – пробел.</p> <p>Замечания:</p> <ul style="list-style-type: none"> <li>• если имя объекта содержит пробел, оно должно быть заключено в кавычки;</li> <li>• если указан конкретный каталог, проверяются все файлы, содержащиеся в нем.</li> </ul>
<b>/discs/</b>	Проверка всех дисков.
<b>/discs/&lt;disc_name&gt;:/&lt;folder&gt;</b>	Проверка указанного диска, где <disc_name> – наименование диска, а <folder> – путь к проверяемому каталогу.
<p><b>&lt;действие&gt;</b> – параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению <b>-i8</b>.</p>	
<b>-i0</b>	Не совершать над объектом никаких действий, только фиксировать информацию о нем в отчете.
<b>-i1</b>	Лечить зараженные объекты, если лечение невозможно – пропустить.
<b>-i2</b>	Лечить зараженные объекты, если лечение невозможно – удалять; не удалять зараженные объекты из контейнеров (составных объектов); удалять контейнеры с исполняемым заголовком (sfx-архивы).
<b>-i3</b>	Лечить зараженные объекты, если лечение невозможно – удалять; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
<b>-i4</b>	Удалять зараженные объекты; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
<b>-i8</b>	Запрашивать действие у пользователя при обнаружении зараженного объекта.
<b>-i9</b>	Запрашивать действие у пользователя по окончании проверки.
<p><b>&lt;типы файлов&gt;</b> – параметр определяет типы файлов, которые будут подвергаться антивирусной проверке. По умолчанию, если параметр не задан, проверяются только заражаемые файлы по содержимому.</p>	

-fe	Проверять только заражаемые файлы по расширению.
-fi	Проверять только заражаемые файлы по содержимому.
-fa	Проверять все файлы.
<b>&lt;исключения&gt;</b> – параметр определяет объекты, исключаемые из проверки. Параметр может включать несколько значений из представленного списка, разделенных пробелом.	
-e:a	Не проверять архивы.
-e:b	Не проверять почтовые базы.
-e:m	Не проверять почтовые сообщения в формате plain text.
-e:<filemask>	Не проверять объекты по маске.
-e:<seconds>	Пропускать объекты, которые проверяются дольше указанного параметром <seconds> времени.
-es:<size>	Пропускать объекты, размер которых (в мегабайтах) превышает значение, заданное параметром <size>.

Примеры:

- Запустить проверку каталога Documents and Settings и диска <D>:

```
SCAN /discs/D: «/discs/C:/Documents and Settings»
```

## ОБНОВЛЕНИЕ АНТИВИРУСА КАСПЕРСКОГО

Команда для обновления баз и программных модулей Антивируса Касперского имеет следующий синтаксис:

```
UPDATE [<источник_обновлений>] [-R[A]:<файл_отчета>]
```

Описание параметров:

<b>&lt;источник_обновлений&gt;</b>	HTTP-, FTP-сервер или сетевой каталог для загрузки обновлений. В качестве значения для данного параметра может быть указан полный путь к источнику обновлений либо url-адрес. Если путь не указан, источник обновлений будет взят из параметров сервиса обновления Антивируса Касперского.
<b>-R[A]:&lt;файл_отчета&gt;</b>	<p><b>-R:&lt;файл_отчета&gt;</b> – фиксировать в отчете только важные события.</p> <p><b>-RA:&lt;файл_отчета&gt;</b> – записывать в отчет все события.</p> <p>Допускается использование абсолютного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.</p>

Примеры:

- Обновить базы, зафиксировав все события в отчете:

```
UPDATE -RA:/discs/C:/avbases_upd.txt
```

## ОТКАТ ПОСЛЕДНЕГО ОБНОВЛЕНИЯ

### Синтаксис команды:

```
ROLLBACK [-R[A]:<файл_отчета>]
```

### Описание параметров:

<b>-R[A]:&lt;файл_отчета&gt;</b>	<p><b>-R:&lt;файл_отчета&gt;</b> – фиксировать в отчете только важные события.</p> <p><b>-RA:&lt;файл_отчета&gt;</b> – записывать в отчет все события.</p> <p>Допускается использование абсолютного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.</p>
----------------------------------	--

### Пример:

```
ROLLBACK -RA:/discs/C:/rollback.txt
```

## ПРОСМОТР СПРАВКИ

Для просмотра справки по синтаксису командной строки предусмотрена команда:

```
[ -? | HELP ]
```

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

```
<команда> -?
```

```
HELP <команда>
```

# ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ АНТИВИРУСА КАСПЕРСКОГО

После установки и настройки Антивируса Касперского вы можете проверить с помощью тестового «вируса» и его модификаций, правильно ли выполнена настройка параметров. Проверку следует выполнять для каждого компонента защиты / протокола отдельно.

## В ЭТОМ РАЗДЕЛЕ

Тестовый «вирус» EICAR и его модификации.....	<a href="#">103</a>
Проверка корректности настройки Файлового Антивируса .....	<a href="#">104</a>
Проверка корректности настройки задачи проверки на вирусы .....	<a href="#">105</a>

## ТЕСТОВЫЙ «ВИРУС» EICAR И ЕГО МОДИФИКАЦИИ

Тестовый «вирус» был специально разработан организацией **eicar** (The European Institute for Computer Antivirus Research) для проверки работы антивирусных продуктов.

Тестовый «вирус» НЕ ЯВЛЯЕТСЯ ВИРУСОМ и не содержит программного кода, который может нанести вред вашему компьютеру, однако при этом большинство продуктов антивирусных компаний-производителей идентифицируют его как вирус.

**Никогда не используйте в качестве проверки работоспособности антивирусного продукта настоящие вирусы!**

Загрузить тестовый «вирус» можно с официального сайта организации **EICAR**: [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

Перед загрузкой необходимо отключить антивирусную защиту, поскольку файл *anti\_virus\_test\_file.htm* будет идентифицирован и обработан программой как зараженный объект, перемещаемый по HTTP-протоколу. Не забудьте включить антивирусную защиту сразу после загрузки тестового «вируса».

Программа идентифицирует файл, загруженный с сайта компании **EICAR** как зараженный объект, содержащий **не подлежащий лечению** вирус, и выполняет действие, установленное для такого объекта.

Вы также можете использовать модификации стандартного тестового «вируса» для проверки работы программы. Для этого следует изменить содержание стандартного «вируса», добавив к нему один из префиксов (см. таблицу далее). Для создания модификаций тестового «вируса» может использоваться любой текстовый или гипертекстовый редактор, например, **Microsoft Блокнот**, **UltraEdit32**, и т.д.

Вы можете проверять корректность работы антивирусной программы с помощью модифицированного «вируса» EICAR только при наличии антивирусных баз, датированных не ранее 24.10.2003 (кумулятивное обновление – Октябрь, 2003).

В первой графе приведены префиксы, которые следует добавить в начало строки стандартного тестового «вируса». Во второй графе перечислены все возможные значения статуса, присваиваемого Антивирусом объекту по результатам проверки. Третья графа содержит информацию об обработке программой объектов с указанным статусом. Обращаем ваше внимание, что действия над объектами определяются значениями параметров программы.

После добавления префикса к тестовому «вирусу» сохраните полученный файл, например, под именем: *ecar\_dele.com*. Дайте аналогичные названия всем модифицированным «вирусам».

Таблица 1. Модификации тестового «вируса»

Префикс	Статус объекта	Информация об обработке объекта
Префикс отсутствует, стандартный тестовый «вирус».	<b>Зараженный.</b> Объект содержит код известного вируса. Лечение невозможно.	Программа идентифицирует данный объект как вирус, не подлежащий лечению.  При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов.
CORR-	<b>Поврежденный.</b>	Программа получила доступ к объекту, но не смогла проверить его, поскольку объект поврежден (например, нарушена структура объекта, неверный формат файла). Информацию о том, что объект был обработан, вы можете найти в отчете о работе программы.
WARN-	<b>Подозрительный.</b> Объект содержит код неизвестного вируса. Лечение невозможно.	Объект признан подозрительным с использованием эвристического анализатора. На момент обнаружения базы Антивируса не содержат описания процедуры лечения данного объекта. Вы получите уведомление при обнаружении такого объекта.
SUSP-	<b>Подозрительный.</b> Объект содержит модифицированный код известного вируса. Лечение невозможно.	Программа обнаружила частичное совпадение участка кода объекта с участком кода известного вируса. На момент обнаружения базы Антивируса не содержат описания процедуры лечения данного объекта. Вы получите уведомление при обнаружении такого объекта.
ERRO-	<b>Ошибка проверки.</b>	При проверке объекта возникла ошибка. Программа не смогла получить доступ к объекту: нарушена целостность объекта (например, нет конца многотомного архива) либо отсутствует связь с ним (если проверяется объект на сетевом ресурсе). Информацию о том, что объект был обработан, вы можете найти в отчете о работе программы.
CURE-	<b>Зараженный.</b> Объект содержит код известного вируса. Излечим.	Объект содержит вирус, который может быть вылечен. Программа выполняет лечение объекта, при этом текст тела «вируса» изменяется на CURE. Вы получите уведомление при обнаружении такого объекта.
DELE-	<b>Зараженный.</b> Объект содержит код известного вируса. Лечение невозможно.	Программа идентифицирует данный объект как вирус, не подлежащий лечению.  При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов.  Вы получите уведомление при обнаружении такого объекта.

## ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ ФАЙЛОВОГО АНТИВИРУСА

► Чтобы проверить, насколько корректно настроен Файловый Антивирус, выполните следующие действия:

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации **EICAR** ([http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)), а также созданные вами модификации тестового «вируса».
2. Разрешите запись в отчет всех событий, чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя.
3. Запустите файл тестового «вируса» или его модификацию на выполнение.



Файловый Антивирус перехватит обращение к файлу, проверит его и выполнит действие, заданное в параметрах. Выбирая различные варианты действий над обнаруженным объектом, вы сможете проверить работу компонента полностью.

Полную информацию о результате работы Файлового Антивируса можно посмотреть в отчете о работе компонента.

## ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ ЗАДАЧИ ПРОВЕРКИ НА ВИРУСЫ

➔ *Чтобы проверить, насколько корректно настроена задача проверки на вирусы, выполните следующие действия:*

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации **EICAR** ([http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)), а также созданные вами модификации тестового «вируса».
2. Создайте новую задачу проверки на вирусы и в качестве объекта проверки выберите папку, содержащую набор тестовых «вирусов».
3. Разрешите запись в отчет всех событий, для того чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя.
4. Запустите задачу проверки на вирусы на выполнение.

При проверке по мере обнаружения подозрительных или зараженных объектов будут выполняться действия, заданные в параметрах задачи. Выбирая различные варианты действий над обнаруженным объектом, вы сможете проверить работу компонента полностью.

Полную информацию о результат выполнения задачи проверки на вирусы можно посмотреть в отчете по работе компонента.

# ВИДЫ УВЕДОМЛЕНИЙ

При возникновении событий в процессе работы Антивируса Касперского на экран выводятся специальные уведомления. В зависимости от степени важности события, с точки зрения безопасности компьютера, уведомления могут быть следующих типов:

- **Тревога.** Произошло событие критической важности, например, обнаружен вредоносный объект или опасная активность в системе. Необходимо немедленно принять решение о дальнейших действиях. Данный тип уведомления имеет красный цвет.
- **Внимание.** Произошло потенциально опасное событие, например, обнаружен возможно зараженный объект или подозрительная активность в системе. Необходимо принять решение, насколько данное событие опасно на ваш взгляд. Данный тип уведомления имеет желтый цвет.
- **Информация.** Уведомление информирует о событии, не имеющем первостепенной важности. Информационные уведомления имеют голубой цвет.

## В ЭТОМ РАЗДЕЛЕ

---

Обнаружен вредоносный объект.....	<a href="#">106</a>
Лечение объекта невозможно .....	<a href="#">107</a>
Обнаружен подозрительный объект .....	<a href="#">107</a>

## ОБНАРУЖЕН ВРЕДОНОСНЫЙ ОБЪЕКТ

При обнаружении Файловым Антивирусом или задачей проверки на вирусы вредоносного объекта на экране открывается специальное уведомление.

Уведомление содержит:

- Вид угрозы (например, *вирус, троянская программа*) и имя вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя вредоносного объекта оформлено в виде ссылки на ресурс [www.viruslist.ru](http://www.viruslist.ru), где вы можете получить подробную информацию о том, угроза какого рода обнаружена на сервере.
- Полное имя вредоносного объекта и путь к нему.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Лечить** – попытаться лечить вредоносный объект. Перед лечением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.
- **Удалить** – удалить вредоносный объект. Перед удалением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.
- **Пропустить** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, лишь зафиксировать информацию о нем в отчете.

Позже вы можете вернуться к обработке пропущенных вредоносных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Для того чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок  **Применить во всех подобных случаях.**

Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи проверки на вирусы от момента запуска до завершения.

## ЛЕЧЕНИЕ ОБЪЕКТА НЕВОЗМОЖНО

В некоторых случаях лечение вредоносного объекта невозможно. Например, если файл поврежден настолько, что удалить из него вредоносный код и восстановить целостность не удастся. Кроме того, процедура лечения не применима к некоторым видам вредоносных объектов, например, троянским программам.

В данных случаях на экран выводится специальное уведомление, которое содержит:

- Вид угрозы (например, *вирус*, *троянская программа*) и имя вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя вредоносного объекта оформлено в виде ссылки на ресурс [www.viruslist.ru](http://www.viruslist.ru), где вы можете получить подробную информацию о том, угроза какого рода обнаружена на вашем компьютере.
- Полное имя вредоносного объекта и путь к нему.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Удалить** – удалить вредоносный объект. Перед удалением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.
- **Пропустить** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, лишь зафиксировать информацию о нем в отчете.

Позже вы можете вернуться к обработке пропущенных вредоносных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок  **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи проверки на вирусы от момента запуска до завершения.

## ОБНАРУЖЕН ПОДОЗРИТЕЛЬНЫЙ ОБЪЕКТ

При обнаружении Файловым Антивирусом или задачей проверки на вирусы объекта, содержащего код неизвестного вируса либо модифицированный код известного вируса, на экране открывается специальное уведомление.

Уведомление содержит:

- Вид угрозы (например, *вирус*, *троянская программа*) и имя объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя вредоносного объекта оформлено в виде ссылки на ресурс [www.viruslist.ru](http://www.viruslist.ru), где вы можете получить подробную информацию о том, угроза какого рода обнаружена на вашем компьютере.
- Полное имя объекта и путь к нему.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Карантин** – поместить объект на карантин. При помещении объекта на карантин выполняется его перемещение, а не копирование: объект удаляется с диска или из почтового сообщения и сохраняется в карантинном каталоге. Файлы на карантине хранятся в специальном формате и не представляют опасности.

При последующих проверках карантина с обновленными сигнатурами угроз статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз. Либо объект получит статус не *заражен*, и его можно будет восстановить.

- **Удалить** – удалить объект. Перед удалением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.
- **Пропустить** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, лишь зафиксировать информацию о нем в отчете.

Позже вы можете вернуться к обработке пропущенных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Для того чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок  **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи проверки на вирусы от момента запуска до завершения.

Если вы уверены, что обнаруженный объект таковым не является, рекомендуется, во избежание повторных срабатываний программы при работе с этим объектом, добавить его в доверенную зону.

# РАБОТА С ПРОГРАММОЙ ИЗ КОМАНДНОЙ СТРОКИ

Вы можете работать с Антивирусом Касперского посредством командной строки.

Синтаксис командной строки:

```
avr.com <команда> [параметры]
```

Обращение к программе через командную строку должно осуществляться из каталога установки Антивируса Касперского либо с указанием полного пути к avr.com.

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 Антивируса Касперского (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
- **START** – запуск компонента или задачи.
- **STOP** – остановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс Антивируса Касперского).
- **STATUS** – вывод на экран текущего статуса компонента или задачи.
- **STATISTICS** – вывод на экран статистики по работе компонента или задачи.
- **EXPORT** – экспорт параметров защиты программы.
- **IMPORT** – импорт параметров защиты Антивируса Касперского (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
- **ACTIVATE** – активация Антивируса Касперского через интернет с помощью кода активации.
- **ADDKEY** – активация программы с помощью файла ключа (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
- **RESTORE** – восстановление файла из карантина.
- **EXIT** – завершение работы с программой (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
- **TRACE** – получение файла трассировки.

Каждой команде соответствует собственный набор параметров, специфичный для конкретного компонента программы.

## В ЭТОМ РАЗДЕЛЕ

Просмотр справки.....	<a href="#">110</a>
Проверка на вирусы .....	<a href="#">110</a>
Обновление программы.....	<a href="#">112</a>
Откат последнего обновления.....	<a href="#">113</a>
Запуск / остановка работы Файлового Антивируса или задачи .....	<a href="#">113</a>
Статистика работы компонента или задачи .....	<a href="#">114</a>
Экспорт параметров защиты .....	<a href="#">115</a>
Импорт параметров защиты .....	<a href="#">115</a>
Активация программы .....	<a href="#">115</a>
Восстановление файла из карантина .....	<a href="#">116</a>
Завершение работы программы.....	<a href="#">116</a>
Получение файла трассировки .....	<a href="#">116</a>
Коды возврата командной строки.....	<a href="#">117</a>

## ПРОСМОТР СПРАВКИ

Для просмотра справки по синтаксису командной строки предусмотрена команда:

```
avp.com [ /? | HELP ]
```

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

```
avp.com <команда> /?
```

```
avp.com HELP <команда>
```

## ПРОВЕРКА НА ВИРУСЫ

Командная строка запуска проверки некоторой области на присутствие вирусов и обработки вредоносных объектов имеет следующий общий вид:

```
avp.com SCAN [<объект проверки>] [<действие>] [<типы файлов>] [<исключения>]
[<параметры отчета>] [<дополнительные параметры>]
```

Для проверки объектов вы также можете воспользоваться сформированными в программе задачами, запустив нужную из командной строки. При этом задача будет выполнена с параметрами, установленными в интерфейсе Антивируса Касперского.

Описание параметров:

**<объект проверки>** – параметр задает перечень объектов, которые будут проверены 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 содержит пробел, оно должно быть заключено в кавычки;
  - если указана конкретная папка, проверяются все файлы, содержащиеся в ней.
- **/ALL** – полная проверка компьютера.
- **/MEMORY** – объекты оперативной памяти.
- **/STARTUP** – объекты автозапуска.
- **/MAIL** – почтовые базы.
- **/REMDRIVES** – все съемные диски.
- **/FIXDRIVES** – все локальные диски.
- **/NETDRIVES** – все сетевые диски.
- **/QUARANTINE** – объекты на карантине.
- **/@:<filelist.lst>** – путь к файлу со списком объектов и каталогов, включаемых в проверку. Файл должен иметь текстовый формат, каждый объект проверки необходимо указывать с новой строки. Допускается ввод абсолютного или относительного пути к файлу. Путь указывается в кавычках, если в нем содержится пробел.

**<действие>** – параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению **/i2**. Возможны следующие значения:

- **/i0** – не совершать над объектом никаких действий, только фиксировать информацию о нем в отчете.
- **/i1** – лечить зараженные объекты, если лечение невозможно – пропустить.
- **/i2** – лечить зараженные объекты, если лечение невозможно – удалять; не удалять зараженные объекты из контейнеров (составных объектов); удалять контейнеры с исполняемым заголовком (sfx-архивы). Данное действие используется по умолчанию.
- **/i3** – лечить зараженные объекты, если лечение невозможно – удалять; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
- **/i4** – удалять зараженные объекты; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
- **/i8** – запрашивать действие у пользователя при обнаружении зараженного объекта.
- **/i9** – запрашивать действие у пользователя по окончании проверки.

**<типы файлов>** – параметр определяет типы файлов, которые будут подвергаться 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.

- **/fa** – проверять все файлы.

**<исключения>** – параметр определяет объекты, исключаемые из проверки. Параметр может включать несколько значений из представленного списка, разделенных пробелом.

- **/e:a** – не проверять архивы.
- **/e:b** – не проверять почтовые базы.
- **/e:m** – не проверять почтовые сообщения в формате plain text.
- **/e:<mask>** – не проверять объекты по маске.
- **/e:<seconds>** – пропускать объекты, которые проверяются дольше указанного параметром **<seconds>** времени.

**<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.

- **/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 технологий антивирусной проверки и файла настроек параметров:

- **/iChecker=<on|off>** – включить / отключить использование технологии iChecker.
- **/iSwift=<on|off>** – включить / отключить использование технологии iSwift.
- **/C:<имя\_конфигурационного\_файла>** – определяет путь к конфигурационному файлу, содержащему параметры работы программы при проверке. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе программы.

Примеры:

- *Запустить проверку оперативной памяти, объектов автозапуска, почтовых баз, а также каталогов My Documents, Program Files и файла test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL «C:\Documents and Settings\All Users\My Documents»
«C:\Program Files» «C:\Downloads\test.exe»
```

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

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Пример конфигурационного файла:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

## ОБНОВЛЕНИЕ ПРОГРАММЫ

Команда для обновления модулей Антивируса Касперского и баз программы имеет следующий синтаксис:

```
avp.com UPDATE [<источник_обновлений>] [/APP=<on|off>] [<параметры_отчета>]
[<дополнительные_параметры>]
```

Описание параметров:



**<источник\_обновлений>** – HTTP-, FTP-сервер или сетевой каталог для загрузки обновлений. Если путь не указан, источник обновлений будет взят из параметров сервиса обновления программы.

**/APP=<on|off>** – включить / отключить 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 проверке. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе программы.

Примеры:

➤ *Обновить базы программы, зафиксировав все события в отчете:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

➤ *Обновить модули Антивируса Касперского, используя параметры конфигурационного файла updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

## ОТКАТ ПОСЛЕДНЕГО ОБНОВЛЕНИЯ

Синтаксис команды:

```
avp.com ROLLBACK </password=<пароль>> [<параметры_отчета>]
```

Описание параметров:

**</password=<пароль>>** – пароль, заданный через интерфейс программы. Без ввода пароля команда ROLLBACK выполняться не будет.

**<параметры отчета>** – параметр, определяющий 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.

- **/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.

Пример:

```
avp.com ROLLBACK/password=123/RA:rollback.txt
```

## ЗАПУСК / ОСТАНОВКА РАБОТЫ ФАЙЛОВОГО АНТИВИРУСА ИЛИ ЗАДАЧИ

Синтаксис команды START:

```
avp.com START <профайл|имя_задачи> [<параметры_отчета>]
```

### Синтаксис команды STOP:

```
avp.com STOP <профайл|имя_задачи> </password=<пароль>>
```

### Описание параметров:

**</password=<пароль>>** – пароль, заданный через интерфейс программы. Без ввода пароля команда STOP выполняться не будет.

**<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:

- **Protection (RTP)** – все компоненты защиты;
- **File\_Monitoring (FM)** – Файловый Антивирус;
- **Scan\_My\_Computer** – задача полной проверки компьютера;
- **Scan\_Objects** – проверка объектов;
- **Scan\_Quarantine** – проверка карантина;
- **Scan\_Startup (STARTUP)** – проверка объектов автозапуска;
- **Updater** – задача обновления;
- **Rollback** – задача отката обновлений.

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

### Примеры:

➡ Чтобы включить Файловый Антивирус, в командной строке введите:

```
avp.com START FM
```

➡ Чтобы остановить задачу полной проверки, в командной строке введите:

```
avp.com STOP SCAN_MY_COMPUTER /password=<ваш_пароль>
```

## СТАТИСТИКА РАБОТЫ КОМПОНЕНТА ИЛИ ЗАДАЧИ

### Синтаксис команды STATUS:

```
avp.com STATUS <профайл|имя_задачи>
```

### Синтаксис команды STATISTICS:

```
avp.com STATISTICS <профайл|имя_задачи>
```

### Описание параметров:

**<профайл|имя\_задачи>** – указывается одно из значений, перечисленных в команде START / STOP (см. стр. [113](#)).

## ЭКСПОРТ ПАРАМЕТРОВ ЗАЩИТЫ

Синтаксис команды:

```
avp.com EXPORT <профайл|имя_задачи> <имя_файла>
```

Описание параметров:

**<профайл|имя\_задачи>** – указывается одно из значений, перечисленных в команде START / STOP (см. стр. [113](#)).

**<имя\_файла>** – путь к файлу, в который экспортируются параметры программы. Может быть указан абсолютный или относительный путь.

Пример:

```
avp.com EXPORT RTP RTP_settings.dat - бинарный формат
avp.com EXPORT FM FM_settings.txt - текстовый формат
```

## ИМПОРТ ПАРАМЕТРОВ ЗАЩИТЫ

Синтаксис команды:

```
avp.com IMPORT <имя_файла> </password=<ваш_пароль>>
```

Описание параметров:

**<имя\_файла>** – путь к файлу, из которого импортируются параметры программы. Может быть указан абсолютный или относительный путь.

**</password=<ваш\_пароль>>** – пароль, заданный через интерфейс программы.

Пример:

```
avp.com IMPORT settings.dat
```

## АКТИВАЦИЯ ПРОГРАММЫ

Активацию Антивируса Касперского возможно произвести двумя способами:

- через интернет с помощью кода активации (команда ACTIVATE);
- с помощью файла ключа (команда ADDKEY).

Синтаксис команды:

```
avp.com ACTIVATE <код_активации> </password=<пароль>>
avp.com ADDKEY <имя_файла> </password=<пароль>>
```

Описание параметров:

**<код активации>** – код активации: xxxxx-xxxxx-xxxxx-xxxxx.

**<имя\_файла>** – файла ключа к программе с расширением .key: xxxxxxxx.key.

`</password=<пароль>>` – пароль, заданный через интерфейс программы.

Пример:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key </password=<пароль>>
```

## ВОССТАНОВЛЕНИЕ ФАЙЛА ИЗ КАРАНТИНА

Синтаксис команды:

```
avp.com RESTORE [/REPLACE] <имя_файла>
```

Описание параметров:

**/REPLACE** – замена существующего файла.

**<имя\_файла>** – имя файла для восстановления.

Пример:

```
avp.com REPLACE C:\eicar.com
```

## ЗАВЕРШЕНИЕ РАБОТЫ ПРОГРАММЫ

Синтаксис команды:

```
avp.com EXIT </password=<пароль>>
```

Описание параметров:

`</password=<пароль>>` – пароль, заданный через интерфейс программы. Без ввода пароля команда выполняться не будет.

## ПОЛУЧЕНИЕ ФАЙЛА ТРАССИРОВКИ

Создание файла трассировки может потребоваться при наличии проблем в работе Антивируса Касперского для более точной их диагностики специалистами Службы технической поддержки.

Синтаксис команды:

```
avp.com TRACE [file] [on|off] [<уровень_трассировки>]
```

Описание параметров:

**[on|off]** – включить / отключить создание файла трассировки.

**[file]** – получить трассировку в виде файла.

**<уровень\_трассировки>** – для параметра допустимо указывать числовое значение в диапазоне от 100 (минимальный уровень, только критические сообщения) до 600 (максимальный уровень, все сообщения).

При обращении в Службу технической поддержки следует указывать необходимый уровень трассировки. Если уровень не был указан, то рекомендуется устанавливать значение 500.

Примеры:

- *Отключить создание файлов трассировки:*

```
avp.com TRACE file off
```

- *Создать файл трассировки с уровнем 500:*

```
avp.com TRACE file on 500
```

## 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 конкретного типа 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 опасные объекты обработаны;
- 102 – обнаружены опасные объекты.

# ИЗМЕНЕНИЕ, ВОССТАНОВЛЕНИЕ ИЛИ УДАЛЕНИЕ ПРОГРАММЫ

Удалить программу вы можете следующими способами:

- с помощью мастера установки программы;
- из командной строки (см. раздел «Удаление программы из командной строки» на стр. [120](#));
- через Kaspersky Administration Kit (см. «Руководство по внедрению Kaspersky Administration Kit»);
- через доменные групповые политики Microsoft Windows Server 2000/2003 (см. раздел «Удаление программы» на стр. [24](#)).

## В ЭТОМ РАЗДЕЛЕ

---

Изменение, восстановление и удаление программы с помощью мастера установки .....	<a href="#">118</a>
Удаление программы из командной строки.....	<a href="#">120</a>

## ИЗМЕНЕНИЕ, ВОССТАНОВЛЕНИЕ И УДАЛЕНИЕ ПРОГРАММЫ С ПОМОЩЬЮ МАСТЕРА УСТАНОВКИ

Восстановление программы полезно проводить в том случае, если вы обнаружили какие-либо ошибки в ее работе вследствие некорректной настройки или повреждения его файлов.

➤ *Для того чтобы перейти к восстановлению исходного состояния программы, установке компонентов Антивируса Касперского, которые не были установлены изначально, или удалению программы,*

1. Вставьте CD-диск с дистрибутивом программы в CD/DVD-ROM-устройство, если установка программы производилась с него. В случае установки Антивируса Касперского из другого источника (папка общего доступа, папка на жестком диске и т.д.) убедитесь, что дистрибутив программы присутствует в данном источнике и у вас есть к нему доступ.
2. Выберите **Пуск** → **Программы** → **Kaspersky Anti-Virus 6.0 для Windows Servers MP4** → **Изменение, восстановление или удаление**.

В результате будет запущена программа установки, которая выполнена в виде мастера. Рассмотрим подробнее шаги по восстановлению, изменению компонентного состава программы и ее удалению.

### ШАГ 1. СТАРТОВОЕ ОКНО ПРОГРАММЫ УСТАНОВКИ

Если вы провели все описанные выше действия, необходимые для восстановления или изменения состава программы, на экране будет открыто приветственное окно программы установки Антивируса Касперского. Для продолжения нажмите на кнопку **Далее**.

### ШАГ 2. ВЫБОР ОПЕРАЦИИ

На данном этапе вам нужно определить, какую именно операцию вы хотите выполнить над программой: вам предлагается изменить компонентный состав программы, восстановить исходное состояние установленных

компонентов или удалить какие-либо компоненты или программу полностью. Для выполнения нужной вам операции нажмите на соответствующую кнопку. Дальнейшее действие программы установки зависит от выбранной операции.

Изменение компонентного состава выполняется аналогично выборочной установке программы, где вы можете указать, какие компоненты вы хотите установить, а также выбрать те, которые хотите удалить.

Восстановление программы производится исходя из установленного компонентного состава. Будут обновлены все файлы тех компонентов, которые были установлены, и для каждого из них будет установлен **Рекомендуемый** уровень обеспечиваемой защиты.

При проведении удаленной деинсталляции Антивируса Касперского 6.0 автоматическая перезагрузка сервера не производится. Однако для полного удаления компонентов программы и дальнейшей корректной работы компьютера рекомендуется произвести перезагрузку вручную.

При удалении программы вы можете выбрать, какие данные, сформированные и используемые в работе программы, вы хотите сохранить на вашем компьютере. Чтобы удалить все данные Антивируса Касперского, выберите вариант  **Удалить программу полностью**. Для сохранения данных вам нужно выбрать вариант  **Сохранить объекты программы** и указать, какие именно объекты не нужно удалять:

- *Информация об активации* – файл ключа, необходимый для работы программы.
- *Базы программы* – полный набор сигнатур опасных программ, вирусов и других угроз, актуальный на дату последнего обновления.
- *Объекты резервного хранилища* – резервные копии удаленных или вылеченных объектов. Такие объекты рекомендуется сохранить для возможности последующего восстановления.
- *Объекты карантина* – объекты, возможно зараженные вирусами или их модификациями. Такие объекты содержат код, который похож на код известного вируса, но однозначно судить об их вредоносности нельзя. Рекомендуется их сохранить, поскольку они могут оказаться незараженными или их излечение будет возможно после обновления сигнатур угроз.
- *Параметры защиты* – значения параметров работы всех компонентов программы.
- *Данные iSwift* – база, содержащая информацию о проверенных объектах файловой системы NTFS. Она позволяет ускорить проверку объектов. Используя данные этой базы, Антивирус Касперского проверяет только те объекты, которые изменились со времени последней проверки.

Если между удалением одной версии Антивируса Касперского и установкой другой достаточно продолжительный промежуток времени, не рекомендуем вам использовать базу iSwift, сохраненную с предыдущей установки программы. За это время на компьютер может проникнуть опасная программа, вредоносные действия которой не будут выявлены при использовании данной базы, и это может привести к заражению компьютера.

Для запуска выбранной операции нажмите на кнопку **Далее**. Запустится процесс копирования необходимых файлов на ваш компьютер или удаления выбранных компонентов и данных.

### ШАГ 3. ЗАВЕРШЕНИЕ ОПЕРАЦИИ ВОССТАНОВЛЕНИЯ, ИЗМЕНЕНИЯ ИЛИ УДАЛЕНИЯ ПРОГРАММЫ

Процесс восстановления, изменения или удаления отображается на экране, после чего вы будете уведомлены о его завершении.

Удаление, как правило, требует последующей перезагрузки компьютера, поскольку это необходимо для учета изменений в системе. Запрос на перезагрузку компьютера будет выведен на экран. Нажмите на кнопку **Да**, чтобы выполнить перезагрузку немедленно. Чтобы перезагрузить компьютер позже вручную, нажмите на кнопку **Нет**.

## УДАЛЕНИЕ ПРОГРАММЫ ИЗ КОМАНДНОЙ СТРОКИ

- Чтобы удалить Антивирус Касперского 6.0 для Windows Servers MP4 из командной строки, выполните команду:

```
msiexec /x <имя_пакета>
```

Будет запущен мастер установки, с помощью которого вы сможете провести процедуру удаления программы.

- Чтобы удалить программу в неинтерактивном режиме без перезагрузки компьютера (перезагрузку следует произвести вручную после удаления), наберите:

```
msiexec /x <имя_пакета> /qn
```

- Чтобы удалить программу в неинтерактивном режиме с последующей перезагрузкой компьютера, наберите:

```
msiexec /x <имя_пакета> ALLOWREBOOT=1 /qn
```

Если при установке программы был задан пароль на запрет удаления программы, при удалении продукта необходимо указать данный пароль, иначе процедура удаления не будет осуществлена.

- Чтобы удалить программу с вводом пароля, подтверждающего право на удаление программы, наберите:

```
msiexec /x <имя_пакета> KLUNINSTPASSWD=***** – для удаления программы в интерактивном режиме;
```

```
msiexec /x <имя_пакета> KLUNINSTPASSWD=***** /qn – для удаления программы в неинтерактивном режиме.
```



# УПРАВЛЕНИЕ ПРОГРАММОЙ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

**Kaspersky Administration Kit** – это система централизованного решения основных административных задач по управлению системой антивирусной безопасности компьютерной сети предприятия, построенной на основе программ, входящих в состав продуктов Kaspersky Open Space Security. Kaspersky Administration Kit поддерживает работу во всех сетевых конфигурациях, использующих протокол TCP/IP.

Программа адресована администраторам корпоративных компьютерных сетей, а также сотрудникам, отвечающим за антивирусную защиту компьютеров в организациях.

Антивирус Касперского 6.0 для Windows Servers MP4 один из продуктов «Лаборатории Касперского», управление которым возможно через собственный интерфейс программы, командную строку (эти способы описаны выше в данной документации) либо посредством программы Kaspersky Administration Kit (если компьютер включен в состав системы удаленного централизованного управления).

Для управления Антивирусом Касперского через Kaspersky Administration Kit выполните следующие действия:

- разверните в сети *Сервер администрирования*;
- установите *Консоль администрирования* на рабочее место администратора (подробнее смотрите Руководство по развертыванию «Kaspersky Administration Kit»);
- на компьютерах сети установите Антивирус Касперского и *Агент администрирования* (входящий в состав Kaspersky Administration Kit). Подробнее об удаленной установке инсталляционного пакета Антивируса Касперского на компьютеры сети смотрите Руководство по развертыванию «Kaspersky Administration Kit».

Перед обновлением версии плагина управления Антивирусом Касперского через Kaspersky Administration Kit завершите работу Консоли администрирования.

Доступ к управлению программой через Kaspersky Administration Kit обеспечивает Консоль администрирования (см. рис. ниже). Она представляет собой стандартный интерфейс, интегрированный в ММС, и позволяет администратору выполнять следующие функции:

- удаленно устанавливать и удалять Антивирус Касперского и *Агент администрирования* на компьютеры сети;
- удаленно настраивать Антивирус Касперского на компьютерах сети;
- обновлять базы и модули Антивируса Касперского;
- осуществлять управление лицензиями для Антивируса Касперского на компьютерах сети;

- просматривать информацию о работе программы на клиентских компьютерах.

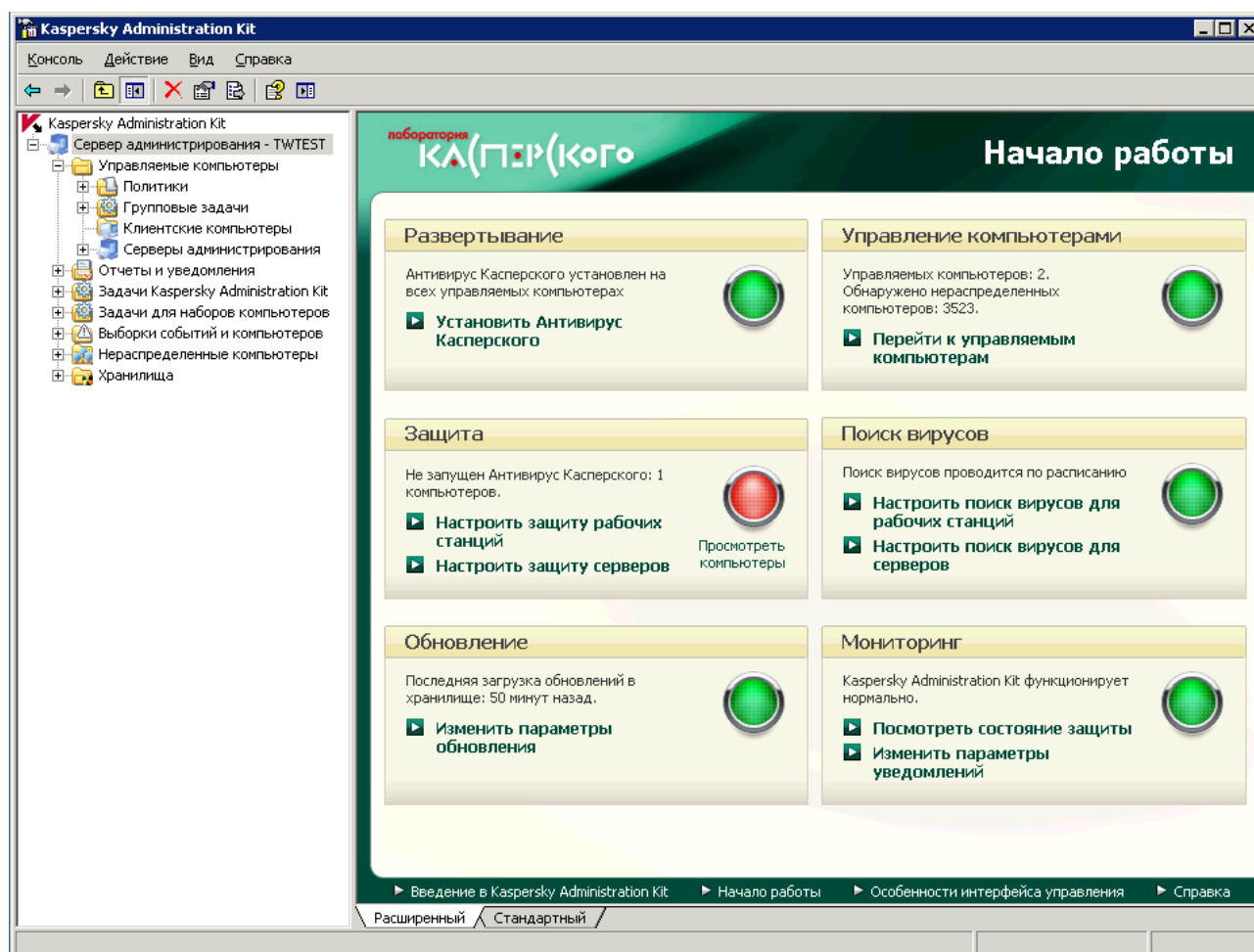


Рисунок 11. Консоль администрирования Kaspersky Administration Kit

Вид главного окна Kaspersky Administration Kit может различаться в зависимости от используемой на компьютере операционной системы.

При работе через Kaspersky Administration Kit управление осуществляется через определение администратором параметров программы, политик и задач.

Именованное действие, выполняемое программой называется *задачей*. В соответствии с выполняемыми функциями задачи разделяют по *типам*: задача проверки на вирусы, задача обновления программы, отката обновлений, задача установки файла ключа.

Каждой задаче соответствует набор параметров работы программы при ее выполнении. Набор параметров работы программы, общий для всех типов его задач, составляет *параметры программы*. Параметры работы программы, специфичные для каждого типа задач, образуют *параметры задачи*. Параметры программы и параметры задач не пересекаются.

Особенностью централизованного управления является организация удаленных компьютеров сети в группы и управление ими через создание и определение групповых политик.

*Политика* – это набор параметров работы программы в группе, а также набор ограничений на переопределение данных параметров при настройке программы или настройке задачи на отдельном клиентском компьютере. Политика включает в себя параметры полной настройки всей функциональности программы, за исключением параметров, индивидуальных для конкретных экземпляров задач. Примером таких параметров являются параметры расписания.

Таким образом, в политику входят параметры:

- общие для всех типов задач – параметры программы;
- общие для всех экземпляров задач каждого типа – большая часть параметров задач.

Это означает, что политика для Антивируса Касперского, в число задач которого входят задачи защиты и проверки на вирусы, включает все необходимые параметры настройки программы при выполнении обоих типов задач, но не включает, например, расписание запуска этих задач, параметры, определяющие область проверки.

## В ЭТОМ РАЗДЕЛЕ

Управление программой .....	<a href="#">123</a>
Управление задачами .....	<a href="#">128</a>
Управление политиками.....	<a href="#">134</a>

## УПРАВЛЕНИЕ ПРОГРАММОЙ

Kaspersky Administration Kit предоставляет возможность удаленного управления запуском и остановкой Антивируса Касперского на отдельном клиентском компьютере, а также настройки общих параметров работы программы: включения и отключения защиты компьютера, настройки параметров отчетов и хранилищ.

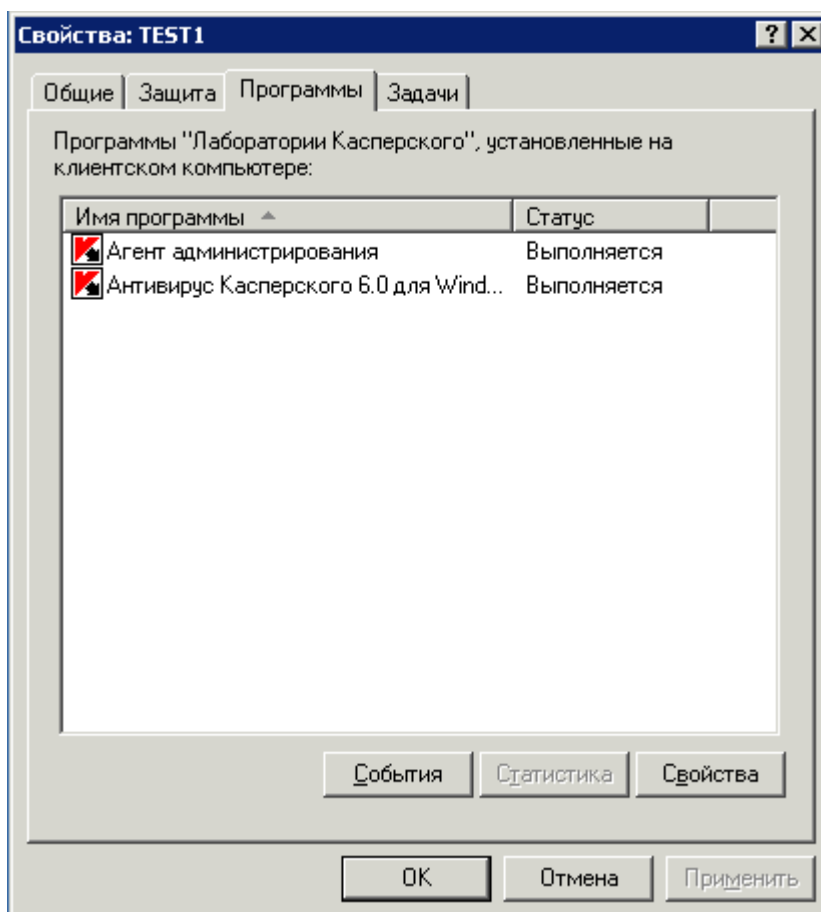


Рисунок 12. Окно свойств клиентского компьютера. Зкладка **Программы**

➡ Чтобы перейти к управлению параметрами программы, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием группы, в состав которой входит клиентский компьютер.
3. В выбранной группе откройте вложенную папку **Клиентские компьютеры** и в панели результатов выберите компьютер, для которого вам необходимо изменить параметры программы.
4. Воспользовавшись командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**, откройте окно свойств клиентского компьютера.
5. В окне свойств клиентского компьютера на закладке **Программы** представлен полный список всех программ «Лаборатории Касперского», установленных на клиентском компьютере. Выберите программу **Антивирус Касперского 6.0 для Windows Servers MP4**.

Под списком программ расположены кнопки управления, с помощью которых вы можете выполнить следующие действия:

- просмотреть список событий в работе программы, произошедших на клиентском компьютере и зарегистрированных на Сервере администрирования;
- просмотреть текущую статистическую информацию о работе программы;
- настроить параметры программы (см. стр. [126](#)).

## ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ

Управление запуском и остановкой Антивируса Касперского 6.0 на удаленном клиентском компьютере осуществляется из окна свойств программы (см. рис. ниже).

В верхней части окна приведены название установленной программы, информация о версии, дата установки, ее статус (запущена или остановлена программа на локальном компьютере), а также информация о состоянии баз программы.

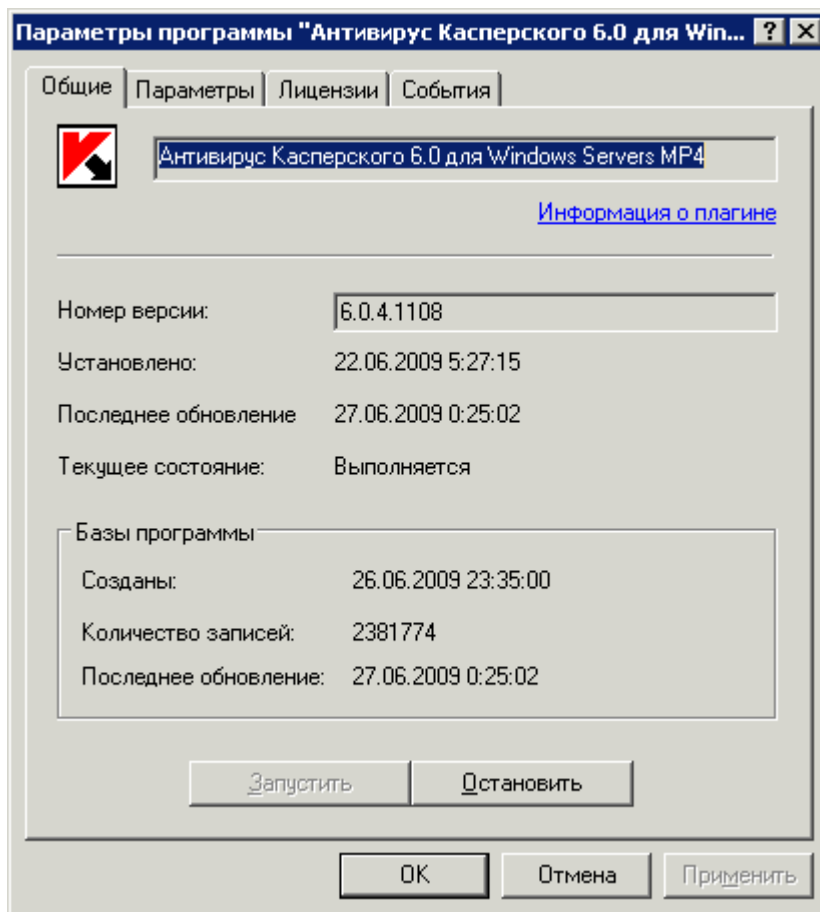


Рисунок 13. Окно свойств программы. Закладка **Общие**

➤ Чтобы остановить или запустить программу на удаленном компьютере, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. стр. [123](#)) на закладке **Программы**.
2. Выберите программу **Антивирус Касперского 6.0 для Windows Servers MP4** и нажмите на кнопку **Свойства**.
3. В открывшемся окне свойств программы на закладке **Общие** нажмите на кнопку **Остановить** для остановки программы или **Запустить** для ее запуска.

## НАСТРОЙКА ПАРАМЕТРОВ ПРОГРАММЫ

Просмотреть и изменить параметры работы программы вы можете в окне свойств программы на закладке **Параметры** (см. рис. ниже). Остальные закладки стандартны для программы Kaspersky Administration Kit, их подробное описание смотрите в одноименном Справочном руководстве.

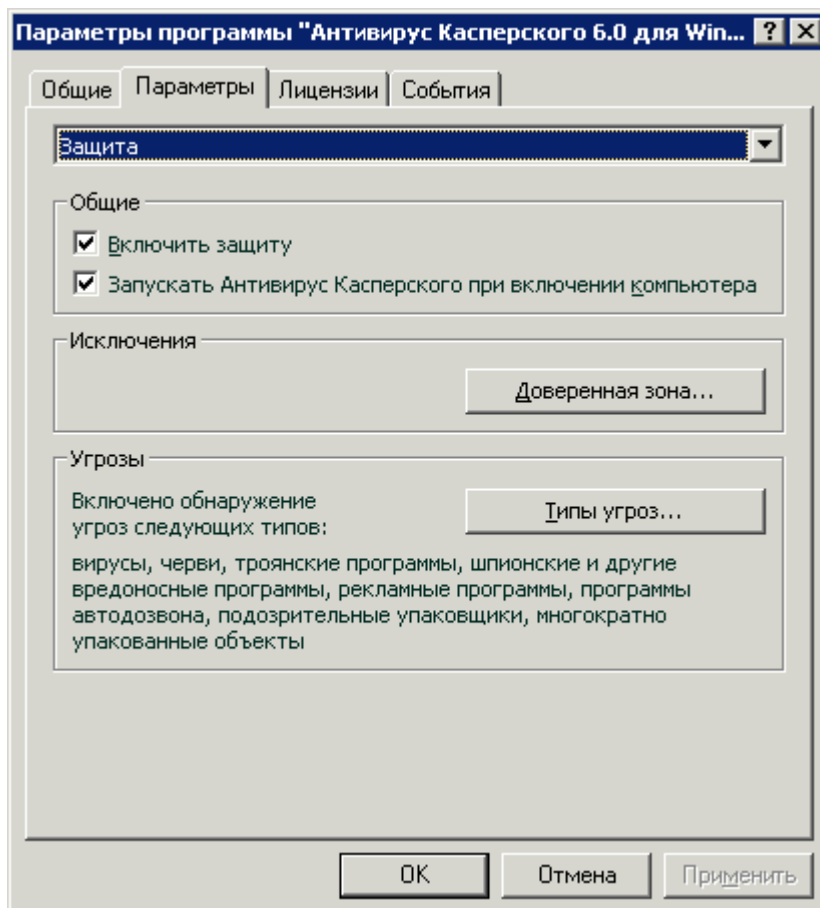


Рисунок 14. Окно свойств программы. Закладка **Параметры**

Если для программы создана политика (см. стр. 135), в которой запрещено переопределение некоторых параметров, то их изменение при настройке параметров программы будет недоступно.

➔ Чтобы перейти к просмотру и изменению параметров работы программы, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. стр. 123) на закладке **Программы**.
2. Выберите программу **Антивирус Касперского 6.0 для Windows Servers MP4** и нажмите на кнопку **Свойства**.
3. В открывшемся окне свойств программы на закладке **Параметры** вы можете настраивать общие параметры работы Антивируса Касперского, параметры отчетов и хранилищ, а также параметры сети. Для этого из раскрывающегося списка в верхней части окна выберите нужное значение и произведите настройку параметров.

**СМ. ТАКЖЕ**

Запуск программы при старте операционной системы .....	<a href="#">77</a>
Выбор категорий обнаруживаемых угроз .....	<a href="#">77</a>
Формирование доверенной зоны .....	<a href="#">78</a>
Настройка отправки уведомлений по электронной почте .....	<a href="#">88</a>

**НАСТРОЙКА СПЕЦИФИЧЕСКИХ ПАРАМЕТРОВ**

При управлении Антивирусом Касперского через Kaspersky Administration Kit вы можете включать или отключать режим взаимодействия программы с пользователем, настраивать внешний вид программы, параметры защиты паролем, а также редактировать информацию о технической поддержке. Настройка этих параметров производится в окне свойств программы (см. рис. ниже).

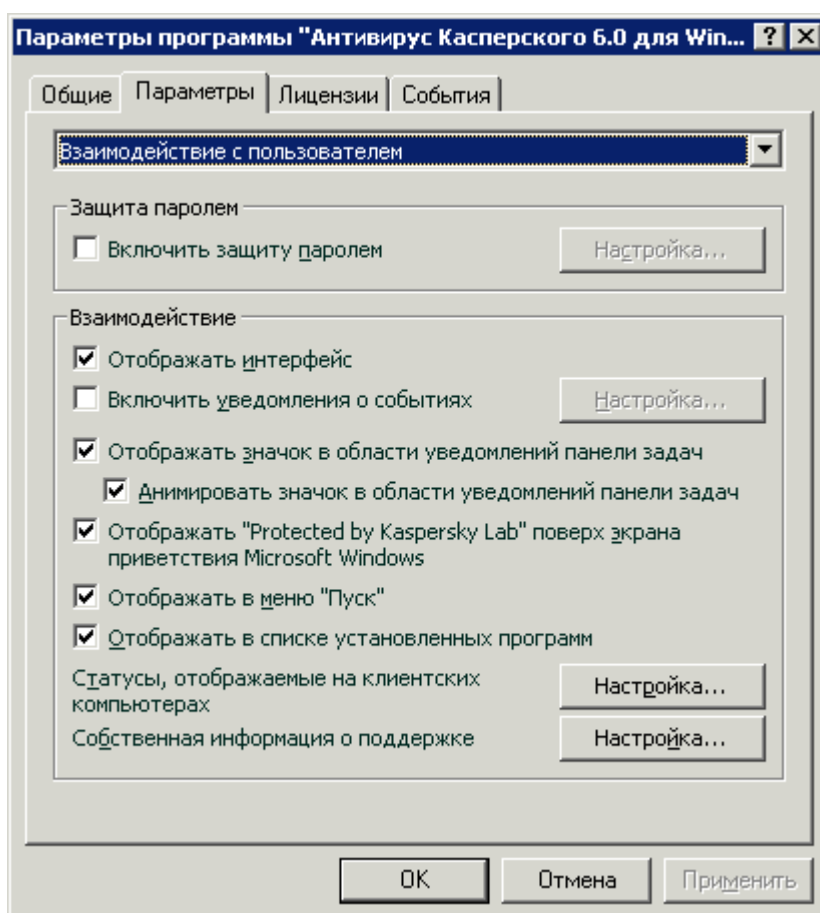


Рисунок 15. Окно свойств программы. Настройка специфических параметров

Чтобы защитить доступ к Антивирусу Касперского с помощью пароля, установите флажок  **Включить защиту паролем** и в окне, открывающемся по кнопке **Настройка**, укажите пароль и область, на которую будет распространяться ограничение доступа.

Для защиты от несанкционированного удаления программы с локального компьютера установите флажок  **Включить защиту от удаления**. В окне, открывающемся по кнопке **Настройка**, укажите пароль на удаление и его подтверждение.

Чтобы защитить доступ к Антивирусу Касперского с помощью пароля, установите флажок  **Включить защиту паролем** и в окне, открываемом по кнопке **Настройка**, укажите пароль и область, на которую будет распространяться ограничение доступа.

Для защиты от несанкционированного удаления программы с локального компьютера установите флажок  **Включить защиту от удаления**. В окне, открываемом по кнопке **Настройка**, укажите пароль на удаление и его подтверждение.

В блоке **Взаимодействие** вы можете указать параметры взаимодействия пользователя с интерфейсом Антивируса Касперского:

- Если флажок  **Запретить взаимодействие с интерфейсом** снят, пользователь, работающий на удаленном компьютере, будет видеть значок Антивируса Касперского, всплывающие сообщения, а также будет иметь возможность принимать решение о дальнейших действиях в окнах уведомлений о наступлении какого-либо события. Для отключения интерактивного режима работы программы установить флажок. Если необходимо скрыть от пользователя факт наличия установленной программы на его компьютере, установите также флажок  **Полностью скрыть наличие установленной программы**.
- В окне **Вид**, открываемом по кнопке **Настройка** вы можете редактировать информацию о технической поддержке пользователей, которая представлена в окне **Поддержка** Антивируса Касперского.

Для изменения информации в верхнем поле введите актуальный текст о предоставляемой поддержке. В поле ниже вы можете редактировать гиперссылки, которые отображаются в блоке **Полезные ссылки** окна **Поддержка**, вызываемого по ссылке **Поддержка** главного окна Антивируса Касперского.

Редактирование списка осуществляется с помощью кнопок **Добавить**, **Изменить**, **Удалить**. Антивирус Касперского добавляет новую ссылку в начало списка. Для изменения порядка следования ссылок в списке воспользуйтесь кнопками **Вверх** и **Вниз**.

Если окно не содержит никаких данных, значит информация о технической поддержке, прописанная по умолчанию, редактированию не подлежит.

В блоке **Статусы программы** вы можете указать статусы программы, которые будут отображаться в главном окне Антивируса Касперского. Для этого нажмите на кнопку **Настройка** и в открывшемся окне установите флажки  рядом с названиями нужных статусов. В этом же окне вы можете указать контрольные периоды баз программы.

В блоке **Вид** вы можете настраивать параметры интерактивного режима работы Антивируса Касперского на удаленном компьютере: отображение уведомления о защите поверх экрана приветствия Microsoft Windows, анимацию значка Антивируса Касперского в системной панели, вывод уведомлений о возникновении событий в работе программы (например, обнаружение опасного объекта).

Если для программы создана политика (см. стр. 135), в которой запрещено переопределение некоторых параметров, то их изменение при настройке параметров программы будет недоступно.

➡ Чтобы перейти к просмотру и изменению специфических параметров работы программы, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. стр. 123) на закладке **Программы**.
2. Выберите программу **Антивирус Касперского 6.0 для Windows Servers MP4** и нажмите на кнопку **Свойства**.
3. В открывшемся окне свойств программы на закладке **Параметры** в раскрываемом списке выберите пункт **Взаимодействие с пользователем** и произведите настройку параметров.

## УПРАВЛЕНИЕ ЗАДАЧАМИ

В данном разделе приведена информация об управлении задачами для Антивируса Касперского. Подробнее о концепции управления задачами через Kaspersky Administration Kit смотрите в одноименном Руководстве администратора.



При установке программы для каждого компьютера сети формируется набор системных задач. В этот список входят задачи защиты (Файловый Антивирус) и проверки на вирусы (Полная проверка, Быстрая проверка) и задачи обновления (обновление баз и модулей программы, откат обновления).

Вы можете управлять запуском системных задач, настраивать их параметры. Удаление данных задач невозможно.

Вы также можете создавать собственные задачи (см. стр. 130), например, задачи проверки, обновления программы и отката обновления, задачу установки файла ключа.

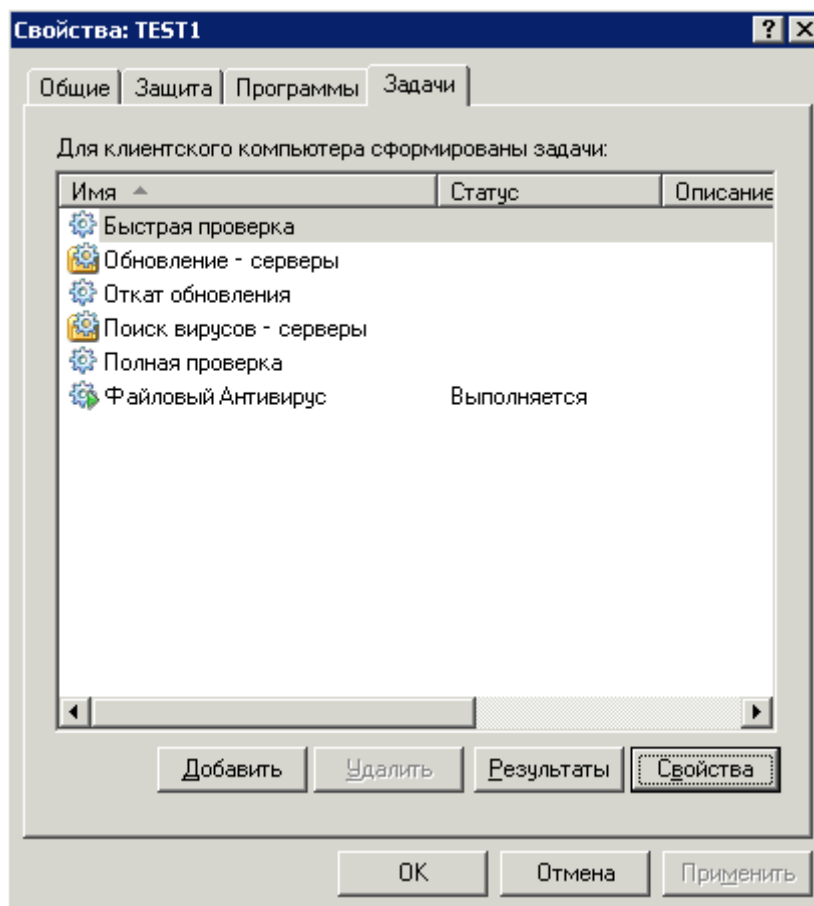


Рисунок 16. Окно свойств клиентского компьютера. Закладка **Задачи**

➤ Для того чтобы открыть список задач, сформированных для клиентского компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration kit.
2. В папке **Управляемые компьютеры** откройте папку с названием группы, в состав которой входит клиентский компьютер.
3. В выбранной группе откройте вложенную папку **Клиентские компьютеры** и в панели результатов выберите компьютер, для которого вам необходимо изменить параметры программы.
4. Воспользовавшись командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**, откройте окно свойств клиентского компьютера.
5. В открывшемся окне свойств клиентского компьютера откройте закладку **Задачи**, на которой представлен полный перечень задач, сформированных для данного клиентского компьютера.

## ЗАПУСК И ОСТАНОВКА ЗАДАЧ

Запуск задач на компьютере выполняется только в том случае, если запущена соответствующая программа (см. стр. 124). При остановке программы выполнение запущенных задач прекращается.

Запуск и остановка задач осуществляется автоматически (в соответствии с расписанием) или вручную (при помощи команд контекстного меню), а также из окна просмотра свойств задачи. Вы можете приостановить процесс выполнения запущенной задачи и возобновить его.

► Чтобы запустить, остановить, приостановить или возобновить действие задачи вручную, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера на закладке **Задачи**.
2. Выберите нужную задачу и откройте ее контекстное меню. Выберите пункт **Запустить** для запуска задачи или пункт **Остановить** – для ее остановки. Можно также воспользоваться аналогичными пунктами в меню **Действие**.

Приостановка и возобновление задачи из контекстного меню невозможно.

или

Выберите в списке нужную задачу и нажмите на кнопку **Свойства**. В открывшемся окне свойств задачи на закладке **Общие** при помощи одноименных кнопок запустите, остановите, приостановите или возобновите действие задачи.

## СОЗДАНИЕ ЗАДАЧИ

При работе с Антивирусом Касперского через Kaspersky Administration Kit вы можете создавать следующие типы задач:

- локальные задачи, определяемые для отдельного клиентского компьютера;
- групповые задачи, определяемые для клиентских компьютеров, входящих в группы администрирования;
- задачи для наборов компьютеров, определяемые для компьютеров вне групп администрирования;
- задачи Kaspersky Administration Kit – специфические задачи Сервера обновления: задачи получения обновлений, задачи резервного копирования и задачи отправки отчетов.

Задачи для наборов компьютеров выполняются только для заданного набора компьютеров. Если в состав группы, для компьютеров которой сформирована задача удаленной установки, будут добавлены новые клиентские компьютеры, для них данная задача выполняться не будет. Необходимо создать новую задачу или внести в настройки параметров уже существующей соответствующие изменения.

Над задачами можно выполнять следующие действия:

- настройку параметров задачи;
- мониторинг выполнения задачи;
- копирование и перенос задачи из одной группы в другую, а также удаление при помощи стандартных команд контекстного меню **Копировать / Вставить**, **Вырезать / Вставить** и **Удалить**, аналогичных пунктов в меню **Действие**.
- импорт и экспорт задач.

Подробные сведения о работе с задачами представлены в Справочном руководстве Kaspersky Administration Kit.

➤ *Чтобы создать локальную задачу, выполните следующие действия:*

1. Откройте окно свойств нужного клиентского компьютера на закладке **Задачи**.
2. Нажмите на кнопку **Добавить**.
3. В результате будет запущен мастер создания новой задачи (см. стр. [131](#)), следуйте его указаниям.

➤ *Чтобы создать групповую задачу, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы.
3. В выбранной группе откройте вложенную папку **Групповые задачи**, в которой будут представлены все созданные для группы задачи.
4. С помощью ссылки **Создать новую задачу** в панели задач запустите мастер создания новой задачи. Информация об особенностях создания групповых задач представлена в Справочном руководстве Kaspersky Administration Kit.

➤ *Чтобы создать задачу для наборов компьютеров (задачу Kaspersky Administration Kit), выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. Выберите папку **Задачи для наборов компьютеров (Задачи Kaspersky Administration Kit)**.
3. С помощью ссылки **Создать новую задачу** в панели задач запустите мастер создания новой задачи. Информация об особенностях создания задач Kaspersky Administration Kit и для наборов компьютеров представлена в Справочном руководстве Kaspersky Administration Kit.

## МАСТЕР СОЗДАНИЯ ЛОКАЛЬНОЙ ЗАДАЧИ

Мастер создания локальной задачи запускается при выборе соответствующего действия в контекстном меню клиентского компьютера или окне его свойств.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Готово**. Для прекращения работы программы на любом этапе служит кнопка **Отмена**.

### ШАГ 1. ВВОД ОБЩИХ ДАННЫХ О ЗАДАЧЕ

Первое окно мастера является вводным: здесь необходимо указать имя задачи (поле **Имя**).

### ШАГ 2. ВЫБОР ПРОГРАММЫ И ТИПА ЗАДАЧИ

На данном этапе следует указать программу, для которой создается задача, – Антивирус Касперского 6.0 для Windows Servers MP4 или Агент администрирования. Кроме того, нужно выбрать тип задачи. Для Антивируса Касперского 6.0 возможно создание следующих задач:

- *Поиск вирусов* – задача проверки на вирусы указанных пользователем областей.
- *Обновление* – задача получения и применения пакета обновлений для программы.
- *Откат обновления* – задача отката последнего произведенного обновления программы.

- *Установка файла ключа* – задача установки файла ключа новой лицензии, необходимой для работы программы.

### ШАГ 3. НАСТРОЙКА ПАРАМЕТРОВ ВЫБРАННОГО ТИПА ЗАДАЧИ

В зависимости от выбранного на предыдущем шаге типа задачи содержимое окна настройки параметров варьируется.

Для задачи проверки на вирусы требуется указать действие (см. стр. 54), которое будет выполнять Антивирус Касперского при обнаружении опасного объекта, а также сформировать список объектов проверки (см. стр. 53).

Для задачи обновления баз и модулей программы требуется указать источник, из которого будут загружены обновления (см. стр. 65). По умолчанию обновление выполняется с сервера обновлений программы Kaspersky Administration Kit.

Задача отката обновлений не имеет специфических настроек.

Для задачи установки файла ключа с помощью кнопки **Обзор** следует указать путь к файлу ключа. Чтобы добавить файл в качестве файла ключа для дополнительной лицензии, установите одноименный флажок . Дополнительная лицензия вступает в силу по окончании срока действия активной лицензии.

Информация о указанной лицензии (номер лицензии, тип и дата окончания) представлена в поле ниже.

### ШАГ 4. НАСТРОЙКА РАСПИСАНИЯ

По завершении настройки параметров задач вам предлагается настроить расписание автоматического запуска задачи.

Для этого в окне настройки расписания выберите из раскрывающегося списка периодичность запуска задачи и в нижней части окна уточните параметры расписания.

### ШАГ 5. ЗАВЕРШЕНИЕ СОЗДАНИЯ ЗАДАЧИ

В последнем окне мастер проинформирует вас об успешном завершении процесса создания задачи.

## НАСТРОЙКА ПАРАМЕТРОВ ЗАДАЧ

Настройка параметров задач программы через интерфейс Kaspersky Administration Kit аналогична настройке через локальный интерфейс Антивируса Касперского, за исключением параметров, которые являются специфическими для данной задачи, например, расписание запуска задач проверки, или параметров, специфичных для Kaspersky Administration Kit, например, параметров, разрешающих (запрещающих) пользователю управлять локальной задачей проверки.

Если для программы создана политика (см. стр. 135), в которой запрещено переопределение некоторых параметров, то их изменение при настройке задач будет недоступно.

Все закладки окна свойств задачи кроме закладки **Параметры** (см. рис. ниже) являются стандартными для программы Kaspersky Administration Kit, их подробное описание смотрите в одноименном справочном руководстве. Закладка **Параметры** содержит специфические параметры Антивируса Касперского, содержимое данной закладки варьируется в зависимости от выбранного типа задачи.

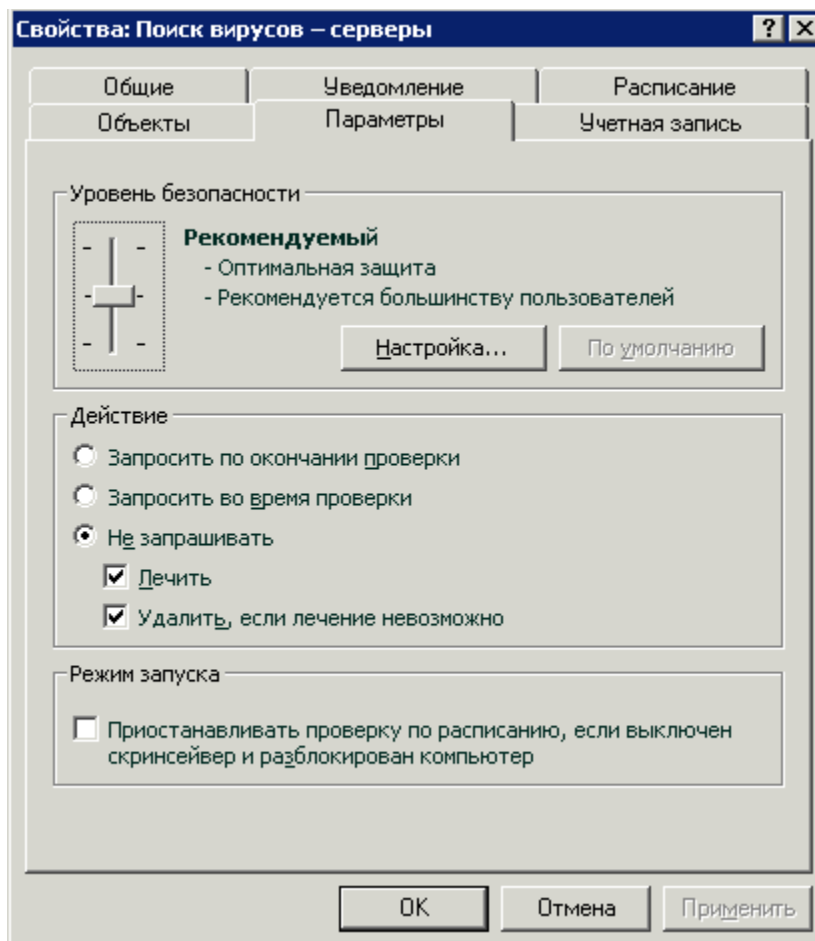


Рисунок 17. Окно свойств задачи. Закладка **Параметры**

➤ Чтобы перейти к просмотру и редактированию локальной задачи, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера на закладке **Задачи**.
2. Выберите задачу в списке и воспользуйтесь кнопкой **Свойства**. В результате будет открыто окно настройки параметров задачи.

➤ Чтобы перейти к групповым задачам, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы.
3. В выбранной группе откройте вложенную папку **Групповые задачи**, в которой будут представлены все созданные для группы задачи.
4. Выберите в дереве консоли нужную задачу для перехода к просмотру и редактированию ее свойств.

В панели задач будет представлена сводная информация о задаче и ссылки для управления выполнением задачи и редактирования ее параметров. Информация об особенностях групповых задач содержится в Справочном руководстве Kaspersky Administration Kit.

➤ Чтобы перейти к задачам для наборов компьютеров (задачам Kaspersky Administration Kit), выполните следующие действия:



1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. Выберите папку **Задачи для наборов компьютеров (Задачи Kaspersky Administration Kit)**.
3. Выберите в дереве консоли нужную задачу для перехода к просмотру и редактированию ее свойств.

В панели задач будет представлена сводная информация о задаче и ссылки для управления выполнением задачи и редактирования ее параметров. Информация об особенностях задач Kaspersky Administration Kit и для наборов компьютеров содержится в Справочном руководстве Kaspersky Administration Kit.

## УПРАВЛЕНИЕ ПОЛИТИКАМИ

Определение политик позволяет распространять единые настройки параметров программы и задач на клиентские компьютеры, входящие в состав одной группы администрирования.

В данном разделе приведена информация о создании и настройке политики для Антивируса Касперского 6.0 для Windows Servers MP4. Более подробную информацию о концепции управления политиками через Kaspersky Administration Kit смотрите в Руководстве администратора к данному продукту.

При создании и настройке политики вы можете налагать запрет на полное или частичное изменение ее параметров в политиках вложенных групп, параметрах задач и параметрах программы. Для этого нажмите на кнопку . Для параметров, запрещенных к изменению, она должна принять вид .

➤ Чтобы открыть список политик, сформированных для Антивируса Касперского, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием группы, в состав которой входит клиентский компьютер.
3. В выбранной группе откройте вложенную папку **Политики**: в дереве консоли будут представлены все созданные для группы политики.

## СОЗДАНИЕ ПОЛИТИКИ

При работе с Антивирусом Касперского через Kaspersky Administration Kit вы можете создавать для него политики.

Над политиками можно выполнять следующие действия:

- настройку параметров политики;
- копирование и перенос политики из одной группы в другую, а также удаление при помощи стандартных команд контекстного меню **Копировать / Вставить**, **Вырезать / Вставить** и **Удалить**, а также аналогичных пунктов в меню **Действие**.
- импорт и экспорт параметров политики.

Более подробная информация о работе с политиками представлена в Справочном руководстве Kaspersky Administration Kit.

➤ Чтобы создать политику, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы.
3. В выбранной группе откройте вложенную папку **Политики**, в которой будут представлены все созданные для группы политики.
4. С помощью ссылки **Создать новую политику** в панели задач запустите мастер создания новой задачи.
5. В открывшемся окне будет запущен мастер создания новой политики (см. стр. [135](#)): следуйте его указаниям.

## МАСТЕР СОЗДАНИЯ ПОЛИТИКИ

Мастер создания политики запускается при выборе соответствующего действия в контекстном меню папки **Политики** нужной группы администрирования или ссылки в панели результатов (для папки **Политики**).

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Готово**. Для прекращения работы программы на любом этапе служит кнопка **Отмена**.

### ШАГ 1. Ввод общих данных о политике

Первые окна мастера являются вводными. Здесь необходимо указать имя политики (поле **Имя**) и выбрать программу **Антивирус Касперского 6.0 для Windows Servers MP4** из раскрывающегося списка **Имя программы**.

Если мастер создания политики был запущен из панели задач узла **Политики** (с помощью ссылки **Создать политику для Антивируса Касперского для Windows Servers MP4**), выбор программы отсутствует.

Если вы хотите создать политику на основании параметров существующей политики для предыдущей версии программы, установите флажок  **Взять параметры из существующей политики** и выберите политику, параметры которой будут использованы в новой политике. Чтобы определить политику, нажмите на кнопку **Выбрать**. В результате будет представлен список существующих политик, которые могут быть использованы при создании политики.

### ШАГ 2. Выбор статуса политики

В данном окне вам предлагается указать статус политики после ее создания, для этого один из вариантов: активная политика, неактивная политика. Подробнее о статусах политик смотрите в Справочном руководстве Kaspersky Administration Kit.

В группе для одной программы может быть создано несколько политик, но действующей (активной) политикой может быть только одна из них.

### ШАГ 3. Импорт параметров программы

Если у вас имеется ранее сохраненный файл с параметрами программы, можно указать его на этом шаге мастера с помощью кнопки **Загрузить**. При этом в следующих окнах мастера будут уже отображать импортированные параметры.

## ШАГ 4. НАСТРОЙКА ПАРАМЕТРОВ ЗАЩИТЫ

На данном этапе вы можете включать (отключать), а также настраивать компоненты защиты, которые будут использоваться в политике.

По умолчанию все компоненты защиты включены. Чтобы отключить какой-либо из них, снимите флажок рядом с его названием. Для детальной настройки компонента защиты выберите его в списке и нажмите на кнопку **Настройка**.

## ШАГ 5. НАСТРОЙКА ЗАЩИТЫ ПАРОЛЕМ

В этом окне мастера вам предлагается настроить параметры защиты паролем на работу с программой и ее удаление.

## ШАГ 6. НАСТРОЙКА ДОВЕРЕННОЙ ЗОНЫ

В этом окне мастера вам предлагается настроить параметры доверенной зоны: добавить в список доверенных программ программное обеспечение, используемое для администрирования сети, и исключить из области проверки некоторые типы файлов.

## ШАГ 7. НАСТРОЙКА ПАРАМЕТРОВ ВЗАИМОДЕЙСТВИЯ С ПОЛЬЗОВАТЕЛЕМ





На данном шаге вы можете указать параметры взаимодействия пользователя с Антивирусом Касперского:

- отображение интерфейса программы на удаленном компьютере;
- уведомление пользователя о событиях;
- отображение значка программы в области уведомлений панели задач и его анимация;
- отображение «Protected by Kaspersky Lab» поверх экрана приветствия Microsoft Windows;
- отображение программы в меню «Пуск»;
- отображение в списке установленных программ.

## ШАГ 8. ЗАВЕРШЕНИЕ СОЗДАНИЯ ПОЛИТИКИ

Последнее окно мастера проинформирует вас об успешном завершении процесса создания политики.

По окончании работы мастера политика для заданной программы будет добавлена в папку **Политики** соответствующей группы администрирования и представлена в дереве консоли.

Для созданной политики вы можете отредактировать ее параметры и установить ограничения на изменения ее параметров с помощью кнопок  и  для каждой группы настроек. При значке  пользователь на клиентском компьютере не сможет изменить настройки. При значке  пользователю доступно редактирование параметров. Распространение политики на клиентские компьютеры будет осуществлено при первой синхронизации клиентов с сервером.



## НАСТРОЙКА ПАРАМЕТРОВ ПОЛИТИКИ

На этапе редактирования вы можете вносить изменения в политику, налагать запрет на изменение параметров в политиках вложенных групп, в параметрах программы и параметрах задач. Параметры политики можно изменять в окне свойств политики (см. рис. ниже).

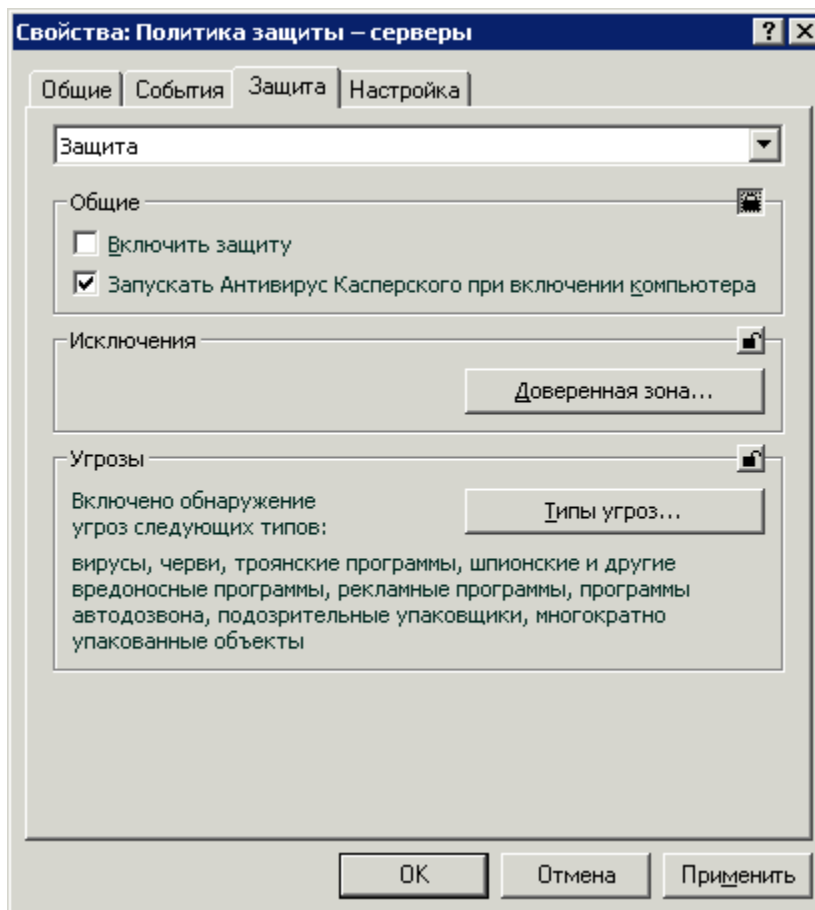


Рисунок 18. Окно свойств политики. Закладка **Защита**

Все закладки (кроме **Защита** и **Настройка**) стандартны для программы Kaspersky Administration Kit. Их подробное описание смотрите в одноименном Руководстве администратора.

Параметры политики для Антивируса Касперского 6.0 включают в себя параметры программы (см. стр. [126](#)) и параметры задач. На закладке **Настройка** представлены параметры программы, а на закладке **Защита** – параметры задач.

Для настройки параметров выберите из раскрывающегося списка в верхней части окна нужное значение и произведите настройку.

➔ *Чтобы перейти к просмотру и настройке параметров политики, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы.
3. В выбранной группе откройте вложенную папку **Политики**, в которой будут представлены все созданные для группы политики.
4. Выберите в дереве консоли нужную политику для перехода к просмотру и редактированию ее свойств.

5. В панели задач будет представлена сводная информация о политике и ссылки для управления статусом политики и редактирования ее параметров.

*или*

Откройте контекстное меню выбранной политики и с помощью пункта **Свойства** откройте окно настройки политики для Антивируса Касперского.

Информация об особенностях работы с политиками содержится в Справочном руководстве Kaspersky Administration Kit.

# ИСПОЛЬЗОВАНИЕ СТОРОННЕГО КОДА

При создании Антивируса Касперского использовался код сторонних производителей.

## В ЭТОМ РАЗДЕЛЕ

---

Библиотека Boost-1.30.0 .....	<a href="#">140</a>
Библиотека LZMA SDK 4.40, 4.43 .....	<a href="#">140</a>
Библиотека Windows Template Library 7.5 .....	<a href="#">140</a>
Библиотека Windows Installer XML (WiX) toolset 2.0 .....	<a href="#">141</a>
Библиотека ZIP-2.31 .....	<a href="#">144</a>
Библиотека ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3 .....	<a href="#">145</a>
Библиотека UNZIP-5.51 .....	<a href="#">145</a>
Библиотека LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12 .....	<a href="#">146</a>
Библиотека LIBJPEG-6B .....	<a href="#">148</a>
Библиотека LIBUNGIF-4.1.4 .....	<a href="#">150</a>
Библиотека MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 .....	<a href="#">150</a>
Библиотека MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 .....	<a href="#">150</a>
Библиотека INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999 .....	<a href="#">150</a>
Библиотека CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004 .....	<a href="#">151</a>
Библиотека COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum .....	<a href="#">151</a>
Библиотека PLATFORM INDEPENDENT IMAGE CLASS .....	<a href="#">151</a>
Библиотека FLEX PARSER (FLEXLEXER)-V. 1993.....	<a href="#">152</a>
Библиотека ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 .....	<a href="#">152</a>
Библиотека STDSTRING- V. 1999.....	<a href="#">153</a>
Библиотека T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006 .....	<a href="#">153</a>
Библиотека NTSERVICE- V. 1997.....	<a href="#">154</a>
Библиотека SHA-1-1.2 .....	<a href="#">154</a>
Библиотека COCOA SAMPLE CODE- V. 18.07.2007 .....	<a href="#">155</a>
Библиотека PUTTY SOURCES-25.09.2008 .....	<a href="#">155</a>
Другая информация.....	<a href="#">156</a>

## БИБЛИОТЕКА Boost-1.30.0

При создании программы использовалась библиотека Boost-1.30.0.

Copyright (C) 2003, Christof Meerwald

---

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the «Software») to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## БИБЛИОТЕКА LZMA SDK 4.40, 4.43

При создании программы использовалась библиотека LZMA SDK 4.40, 4.43.

## БИБЛИОТЕКА WINDOWS TEMPLATE LIBRARY 7.5

При создании программы использовалась библиотека Windows Template Library 7.5.

Copyright (C) 2006, Microsoft Corporation

---

Microsoft Public License (Ms-PL)

Published: October 12, 2006

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

### 1. Definitions

The terms «reproduce», «reproduction», «derivative works», and «distribution» have the same meaning here as under U.S. copyright law.

A «contribution» is the original software, or any additions or changes to the software.

A «contributor» is any person that distributes its contribution under this license.

«Licensed patents» are a contributor's patent claims that read directly on its contribution.

## 2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

## 3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed «as-is.» You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

# БИБЛИОТЕКА WINDOWS INSTALLER XML (WiX) TOOLSET 2.0

При создании программы использовалась библиотека Windows Installer XML (WiX) toolset 2.0.

Copyright (C) 2009, Microsoft Corporation

-----  
Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE («AGREEMENT»). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

## 1. DEFINITIONS

«Contribution» means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
  - i) changes to the Program, and
  - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of

software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

«Contributor» means any person or entity that distributes the Program.

«Licensed Patents» mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

«Program» means the Contributions distributed in accordance with this Agreement.

«Recipient» means anyone who receives the Program under this Agreement, including all Contributors.

## 2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

## 3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

#### 4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor («Commercial Contributor») hereby agrees to defend and indemnify every other Contributor («Indemnified Contributor») against any losses, damages and costs (collectively «Losses») arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

#### 5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN «AS IS» BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

#### 6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### 7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

## БИБЛИОТЕКА ZIP-2.31

При создании программы использовалась библиотека Zip-2.31.

Copyright (C) 1990-2005, Info-ZIP

-----  
This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at

<ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, «Info-ZIP» is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided «as is,» without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names «Info-ZIP» (or any variation thereof, including, but not limited to, different capitalizations), «Pocket UnZip,» «WiZ» or «MacZip» without the explicit permission



of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names «Info-ZIP,» «Zip,» «UnZip,» «UnZipSFX,» «WiZ,» «Pocket UnZip,» «Pocket Zip,» and «MacZip» for its own source and binary releases.

## **БИБЛИОТЕКА ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3**

При создании программы использовалась библиотека Zlib-1.0.4, ZLIB-1.0.8, Zlib-1.1.3, Zlib-1.2.3.

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

-----  
This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

## **БИБЛИОТЕКА UNZIP-5.51**

При создании программы использовалась библиотека UnZip-5.51.

Copyright (c) 1990-2004, Info-ZIP

-----  
This is version 2004-May-22 of the Info-ZIP copyright and license.

The definitive version of this document should be available at <ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, «Info-ZIP» is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided «as is,» without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered

versions with the names «Info-ZIP» (or any variation thereof, including, but not limited to, different capitalizations), «Pocket UnZip,» «WiZ» or «MacZip» without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names «Info-ZIP,» «Zip,» «UnZip,» «UnZipSFX,» «WiZ,» «Pocket UnZip,» «Pocket Zip,» and «MacZip» for its own source and binary releases.

## **БИБЛИОТЕКА LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12**

При создании программы использовалась библиотека libpng-1.0.1, libpng-1.2.8, libpng-1.2.12.

-----  
 This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 1.2.6, August 15, 2004, through 1.2.39, August 13, 2009, are

Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, «Contributing Authors» is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied «AS IS». The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.
3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A «png\_get\_copyright» function is available, for convenient use in «about» boxes and the like:

```
printf(«%s»,png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files «pngbar.png» and «pngbar.jpg» (88x31) and «pngnow.png» (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

August 13, 2009

## БИБЛИОТЕКА LIBJPEG-6B

При создании программы использовалась библиотека libjpeg-6b.

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

-----  
LEGAL ISSUES

=====

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided «AS IS», and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this

README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that «this software is based in part on the work of the Independent JPEG Group».

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as «the Independent JPEG Group's software».

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script «configure» was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium

but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce «uncompressed GIFs». This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

«The Graphics Interchange Format(c) is the Copyright property of

CompuServe Incorporated. GIF(sm) is a Service Mark property of

CompuServe Incorporated.»

## **БИБЛИОТЕКА LIBUNGIF-4.1.4**

При создании программы использовалась библиотека libungif-4.1.4.

Copyright (C) 1997, Eric S. Raymond

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the «Software»), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## **БИБЛИОТЕКА MD5 MESSAGE-DIGEST ALGORITHM-REV. 2**

При создании программы использовалась библиотека MD5 MESSAGE-DIGEST ALGORITHM-REV. 2.

## **БИБЛИОТЕКА MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004**

При создании программы использовалась библиотека MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004.

## **БИБЛИОТЕКА INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999**

При создании программы использовалась библиотека Independent implementation of MD5 (RFC 1321)-v. 04.11.1999.

Copyright (C) 1991-2, RSA Data Security, Inc.

---

RSA's MD5 disclaimer

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the «RSA Data Security, Inc. MD5 Message-Digest Algorithm» in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as «derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm» in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided «as is» without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

## **БИБЛИОТЕКА CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004**

При создании программы использовалась библиотека Conversion routines between UTF32, UTF-16, and UTF-8-v. 02.11.2004.

Copyright 2001-2004 Unicode, Inc.

---

### Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

### Limitations on Rights to Redistribute This Code

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

## **БИБЛИОТЕКА COOL OWNER DRAWN MENUS-V. 2.4, 2.63 BY BRENT CORKUM**

При создании программы использовалась библиотека Cool Owner Drawn Menus-v. 2.4, 2.63 By Brent Corkum.

---

You are free to use/modify this code but leave this header intact. This class is public domain so you are free to use it any of your applications (Freeware, Shareware, Commercial). All I ask is that you let me know so that if you have a real winner I can brag to my buddies that some of my code is in your app. I also wouldn't mind if you sent me a copy of your application since I like to play with new stuff.

Brent Corkum, corkum@rocscience.com

## **БИБЛИОТЕКА PLATFORM INDEPENDENT IMAGE CLASS**

При создании программы использовалась библиотека Platform Independent Image Class.

Copyright (C) 1995, Alejandro Aguilar Sierra (asierra@servidor.unam.mx)

---

Covered code is provided under this license on an «as is» basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

## **БИБЛИОТЕКА FLEX PARSER (FLEXLEXER)-V. 1993**

При создании программы использовалась библиотека Flex parser (FlexLexer)-v. 1993.

Copyright (c) 1993 The Regents of the University of California

---

This code is derived from software contributed to Berkeley by

Kent Williams and Tom Epperly.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: ``This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

## **БИБЛИОТЕКА ENSURECLEANUP, SWMRG, LAYOUT-V. 2000**

При создании программы использовалась библиотека EnsureCleanup, SWMRG, Layout-v. 2000.

Copyright (C) 2009, Microsoft Corporation

---



NOTICE SPECIFIC TO SOFTWARE AVAILABLE ON THIS WEB SITE.

All Software is the copyrighted work of Microsoft and/or its suppliers. Use of the Software is governed by the terms of the end user license agreement, if any, which accompanies or is included with the Software («License Agreement»).

If Microsoft makes Software available on this Web Site without a License Agreement, you may use such Software to design, develop and test your programs to run on Microsoft products and services.

If Microsoft makes any code marked as «sample» available on this Web Site without a License Agreement, then that code is licensed to you under the terms of the Microsoft Limited Public License <http://msdn.microsoft.com/en-us/cc300389.aspx#MLPL>.

The Software is made available for download solely for use by end users according to the License Agreement or these TOU. Any reproduction or redistribution of the Software not in accordance with the License Agreement or these TOU is expressly prohibited.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities («U.S. Government»), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

## БИБЛИОТЕКА STDSTRING- V. 1999

При создании программы использовалась библиотека StdString- v. 1999.

Copyright (C) 1999, Joseph M. O'Leary

-----  
This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes

your \$30 billion dollar satellite explode in orbit. If you redistribute

it in any form, I'd appreciate it if you would leave this notice here.

## БИБЛИОТЕКА T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006

При создании программы использовалась библиотека T-Rex (tiny regular expression library)- v. 2003-2006.

Copyright (C) 2003-2006, Alberto Demichelis

-----

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

## БИБЛИОТЕКА NTSERVICE- V. 1997

При создании программы использовалась библиотека NTService- v. 1997.

Copyright (C) 1997, Joerg Koenig and the ADG mbH, Mannheim, Germany

-----  
Distribute freely, except: don't remove my name from the source or documentation (don't take credit for my work), mark your changes (don't get me blamed for your possible bugs), don't alter or remove this notice.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc., and I'll try to keep a version up to date. I can be reached as follows:

J.Koenig@adg.de (company site)

Joerg.Koenig@rhein-neckar.de (private site)

MODIFIED BY TODD C. WILSON FOR THE ROAD RUNNER NT LOGIN SERVICE.

HOWEVER, THESE MODIFICATIONS ARE BROADER IN SCOPE AND USAGE AND CAN BE USED IN OTHER PROJECTS WITH NO CHANGES.

MODIFIED LINES FLAGGED/BRACKETED BY «//!! TCW MOD»

## БИБЛИОТЕКА SHA-1-1.2

При создании программы использовалась библиотека SHA-1-1.2.

Copyright (C) 2001, The Internet Society

-----  
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an «AS IS» basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## **БИБЛИОТЕКА COCOA SAMPLE CODE- V. 18.07.2007**

При создании программы использовалась библиотека Cocoa sample code- v. 18.07.2007.

Copyright (C) 2007, Apple Inc

-----  
Disclaimer: IMPORTANT: This Apple software is supplied to you by Apple Inc. («Apple»)

in consideration of your agreement to the following terms, and your use, installation, modification or redistribution of this Apple software constitutes acceptance of these terms. If you do not agree with these terms, please do not use, install, modify or redistribute this Apple software.

In consideration of your agreement to abide by the following terms, and subject to these terms, Apple grants you a personal, non – exclusive license, under Apple's copyrights in this original Apple software ( the «Apple Software» ), to use, reproduce, modify and redistribute the Apple Software, with or without modifications, in source and / or binary forms; provided that if you redistribute the Apple Software in its entirety and without modifications, you must retain this notice and the following text and disclaimers in all such redistributions of the Apple Software. Neither the name, trademarks, service marks or logos of Apple Inc. may be used to endorse or promote products derived from the Apple Software without specific prior written permission from Apple. Except as expressly stated in this notice, no other rights or licenses, express or implied, are granted by Apple herein, including but not limited to any patent rights that may be infringed by your derivative works or by other works in which the Apple Software may be incorporated.

The Apple Software is provided by Apple on an «AS IS» basis.

APPLE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON - INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE APPLE SOFTWARE OR ITS USE AND OPERATION ALONE OR IN COMBINATION WITH YOUR PRODUCTS.

IN NO EVENT SHALL APPLE BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES ( INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION ) ARISING IN ANY WAY OUT OF THE USE, REPRODUCTION, MODIFICATION AND / OR DISTRIBUTION OF THE APPLE SOFTWARE, HOWEVER CAUSED AND WHETHER UNDER THEORY OF CONTRACT, TORT ( INCLUDING NEGLIGENCE ), STRICT LIABILITY OR OTHERWISE, EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## **БИБЛИОТЕКА PUTTY SOURCES-25.09.2008**

При создании программы использовалась библиотека PUTTY SOURCES-25.09.2008. Copyright (C) 1997-2009, Simon Tatham.

The PuTTY executables and source code are distributed under the MIT licence, which is similar in effect to the BSD licence. (This licence is Open Source certified <http://www.opensource.org/licenses/> and complies with the Debian Free Software Guidelines [http://www.debian.org/social\\_contract](http://www.debian.org/social_contract))

The precise licence text, as given in the About box and in the file LICENCE in the source distribution, is as follows:

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the «Software»), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

## ДРУГАЯ ИНФОРМАЦИЯ

Для проверки электронной цифровой подписи используется программная библиотека защиты информации (ПБЗИ) «Крипто-Си», разработанная ООО «КриптоЭкс», <http://www.cryptoex.ru>.

Для проверки электронной цифровой подписи используется программная библиотека защиты информации (ПБЗИ) «Агава-С», разработанная ООО «Р-Альфа».

Данный продукт содержит или может содержать программы, которые лицензируются (или сублицензируются) Пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают Пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду («ПО с открытым исходным кодом»). Если такая лицензия предусматривает предоставление исходного кода Пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса на адрес [source@kaspersky.com](mailto:source@kaspersky.com) или сопровождается с продуктом.

# ГЛОССАРИЙ ТЕРМИНОВ

## Ч

### **«ЧЕРНЫЙ» СПИСОК ФАЙЛОВ КЛЮЧЕЙ**

База данных, содержащая информацию о заблокированных «Лабораторией Касперского» файлах ключей, владельцы которых нарушили условия лицензионного соглашения, и о файлах ключей, которые были выписаны, но по какой-либо причине не были проданы либо были заменены. Файл «черного» списка необходим для работы программ «Лаборатории Касперского». Содержимое файла обновляется вместе с базами.

## В

### **ВООТ-ВИРУС (ЗАГРУЗОЧНЫЙ)**

Вирус, поражающий загрузочные секторы дисков компьютера. Вирус «заставляет» систему при ее перезапуске считывать в память и отдавать управление не оригинальному коду загрузчика, а коду вируса.

## О

### **OLE-ОБЪЕКТ**

Присоединенный или встроенный в другой файл объект. Программа «Лаборатории Касперского» позволяет проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

## А

### **АКТИВНАЯ ЛИЦЕНЗИЯ**

Лицензия, используемая в данный временной период для работы программы «Лаборатории Касперского». Лицензия определяет срок действия полной функциональности и лицензионную политику в отношении программы. В программе не может быть больше одной лицензии со статусом «активная».

### **АРХИВ**

Файл, «содержащий» в себе один или несколько других объектов, которые в свою очередь также могут быть архивами.

## Б

### **БАЗЫ**

Базы данных, формируемые специалистами «Лаборатории Касперского» и содержащие подробное описание всех существующих на текущий момент угроз компьютерной безопасности, способов их обнаружения и обезвреживания. Базы постоянно обновляются в «Лаборатории Касперского» по мере появления новых угроз. Для повышения качества обнаружения угроз мы рекомендуем регулярно копировать обновления баз с серверов обновлений «Лаборатории Касперского».

### **БЛОКИРОВАНИЕ ОБЪЕКТА**

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

## В

### **ВИРУСНАЯ АТАКА**

Ряд целенаправленных попыток заразить компьютер вирусом.

### **ВОЗМОЖНО ЗАРАЖЕННЫЙ ОБЪЕКТ**

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Возможно зараженные файлы обнаруживаются с помощью эвристического анализатора.

## **ВОССТАНОВЛЕНИЕ**

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

## **Д**

### **ДОВЕРЕННЫЙ ПРОЦЕСС**

Программный процесс, файловые операции которого не контролируются программой «Лаборатории Касперского» в режиме постоянной защиты. То есть все объекты, запускаемые, открываемые и сохраняемые доверенным процессом, не проверяются.

### **ДОПОЛНИТЕЛЬНАЯ ЛИЦЕНЗИЯ**

Лицензия, добавленная для работы программы «Лаборатории Касперского», но не активированная. Дополнительная лицензия начинает действовать по окончании срока действия активной лицензии.

### **ДОСТУПНОЕ ОБНОВЛЕНИЕ**

Пакет обновлений модулей программы «Лаборатории Касперского», в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

## **З**

### **ЗАГОЛОВОК**

Информация, которая содержится в начале файла или сообщения и состоит из низкоуровневых данных о статусе и обработке файла (сообщения). В частности, заголовок сообщения электронной почты содержит такие сведения, как данные об отправителе, получателе и дату.

### **ЗАГРУЗОЧНЫЙ СЕКТОР ДИСКА**

Загрузочный сектор — это особый сектор на жёстком диске компьютера, дискете или другом устройстве хранения информации. Содержит сведения о файловой системе диска и программу-загрузчик, отвечающую за запуск операционной системы.

Существует ряд вирусов, поражающих загрузочные секторы дисков, которые так и называются – загрузочные вирусы (boot-вирусы). Программа «Лаборатории Касперского» позволяет проверять загрузочные секторы на присутствие вирусов и лечить их в случае заражения.

### **ЗАРАЖЕННЫЙ ОБЪЕКТ**

Объект, внутри которого содержится вредоносный код: при проверке объекта было обнаружено полное совпадение участка кода объекта с кодом известной угрозы. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами, поскольку это может привести к заражению вашего компьютера.

## **И**

### **ИСКЛЮЧЕНИЕ**

Исключение - объект исключаемый из проверки программой «Лаборатории Касперского». Исключать из проверки можно файлы определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по типу угрозы согласно классификации Вирусной энциклопедии. Для каждой задачи могут быть заданы свои исключения.

## **К**

### **КАРАНТИН**

Определенная папка, куда помещаются все возможно зараженные объекты, обнаруженные во время проверки или в процессе функционирования постоянной защиты.

### **КОНТРОЛИРУЕМЫЙ ОБЪЕКТ**

Файл, перемещаемый по протоколам HTTP, FTP или SMTP через межсетевой экран и направляемый на проверку программе «Лаборатории Касперского».

**Л****ЛЕЧЕНИЕ ОБЪЕКТОВ**

Способ обработки зараженных объектов, в результате которого происходит полное или частичное восстановление данных, либо принимается решение о невозможности лечения объектов. Лечение объектов выполняется на основе записей баз. В случае, если лечение является первичным действием над объектом (самое первое действие над объектом сразу после его обнаружения), то перед его выполнением создается резервная копия объекта. В процессе лечения часть данных может быть потеряна. Вы можете использовать эту копию для восстановления объекта до предшествующего лечению состояния.

**ЛЕЧЕНИЕ ОБЪЕКТОВ ПРИ ПЕРЕЗАГРУЗКЕ**

Способ обработки зараженных объектов, используемых в момент лечения другими программами. Заключается в создании копии зараженного объекта, лечении созданной копии и замене при следующей перезагрузке исходного зараженного объекта его вылеченной копией.

**ЛОЖНОЕ СРАБАТЫВАНИЕ**

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

**М****МАКСИМАЛЬНАЯ ЗАЩИТА**

Уровень безопасности вашего компьютера, соответствующий максимально полной защите, которую может обеспечить программа. При таком уровне защиты на присутствие вирусов проверяются все файлы компьютера, сменных носителей и сетевых дисков, если таковые подключены к компьютеру.

**МАСКА ПОДСЕТИ**

Маска подсети (также именуемая сетевой маской) и сетевой адрес определяют адреса входящих в состав сети компьютеров.

**МАСКА ФАЙЛА**

Представление имени и расширения файла общими символами. Двумя основными символами, используемыми в масках файлов, являются \* и ? (где \* – любое число символов, а ? – любой один символ). При помощи данных знаков можно представить любой файл. Обратите внимание, что имя и расширение файла всегда пишутся через точку.

**Н****НЕИЗВЕСТНЫЙ ВИРУС**

Новый вирус, информации о котором нет в базах. Как правило, неизвестные вирусы обнаруживаются программой в объектах при помощи эвристического анализатора, и таким объектам присваивается статус возможно зараженных.

**НЕСОВМЕСТИМАЯ ПРОГРАММА**

Антивирусная программа стороннего производителя или программа «Лаборатории Касперского», не поддерживающая управление через Антивирус Касперского.

**О****ОБНОВЛЕНИЕ**

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

**ОБНОВЛЕНИЕ БАЗ**

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

## ОБЪЕКТЫ АВТОЗАПУСКА

Набор программ, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

## ОПАСНЫЙ ОБЪЕКТ

Объект, внутри которого содержится вирус. Не рекомендуется работать с такими объектами, поскольку это может привести к заражению компьютера. При обнаружении зараженного объекта рекомендуется лечить его с помощью программы «Лаборатории Касперского» или удалить, если лечение невозможно.

## П

### ПАКЕТ ОБНОВЛЕНИЙ

Пакет файлов для обновления программного обеспечения, который копируется из интернета и устанавливается на вашем компьютере.

### ПАПКА ДАННЫХ

Папка размещения необходимых для работы программы служебных папок и баз данных. В случае смены папки данных, вся входящая в ее состав информация должна быть сохранена по новому адресу.

### ПЕРЕХВАТЧИК

Подкомпонент программы, отвечающий за проверку определенных типов почтовых сообщений. Набор подлежащих установке перехватчиков зависит от того, в какой роли или в какой комбинации ролей развернута программа.

### ПОДОЗРИТЕЛЬНЫЙ ОБЪЕКТ

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Подозрительные объекты обнаруживаются при помощи эвристического анализатора.

### ПОМЕЩЕНИЕ ОБЪЕКТОВ НА КАРАНТИН

Способ обработки возможно зараженного объекта, при котором доступ к объекту блокируется, и он перемещается из исходного местоположения в папку карантина, где сохраняется в закодированном виде, что исключает угрозу заражения. Помещенные на карантин объекты могут быть проверены с использованием обновленных баз Антивируса, проанализированы администратором или отправлены в «Лабораторию Касперского».

### ПОРОГ ВИРУСНОЙ АКТИВНОСТИ

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

### ПОСТОЯННАЯ 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 подозреваемые на наличие угрозы, обрабатываются в соответствии с параметрами задачи (лечатся, удаляются, помещаются на карантин).

### ПОТЕНЦИАЛЬНО ЗАРАЖАЕМЫЙ ОБЪЕКТ

Объект, который в силу своей структуры или формата может быть использован злоумышленниками в качестве «контейнера», для размещения и распространения вредоносного объекта. Как правило, это исполняемые файлы, например, с расширением **com**, **exe**, **dll** и др. Риск внедрения в такие файлы вредоносного кода достаточно.



**ПРОВЕРКА ПО ТРЕБОВАНИЮ**

Режим работы программы «Лаборатории Касперского», который инициируется пользователем и направлен на проверку любых файлов.

**ПРОВЕРКА ХРАНИЛИЩ**

Проверка хранящихся на почтовом сервере сообщений и содержимого общих папок с использованием последней версии баз. Проверка осуществляется в фоновом режиме и может запускаться как по расписанию, так и вручную. Проверяются все общие папки и почтовые хранилища (mailbox storage). При проверке могут быть обнаружены новые вирусы, информация о которых отсутствовала в базах на момент предыдущих проверок.

**ПРОПУСК ОБЪЕКТА**

Способ обработки, при котором объект пропускается пользователю без каких-либо изменений. Если параметрами отчета задано протоколирование событий данного типа, информация об обнаруженном объекте заносится в отчет.

**ПРОСТОЙ ОБЪЕКТ**

Тело письма или простое вложение, например, в виде исполняемого файла. См. также объект-контейнер.

**Р****РЕЗЕРВНОЕ КОПИРОВАНИЕ**

Создание резервной копии файла перед его лечением или удалением и размещение этой копии в резервном хранилище с возможностью последующего восстановления файла, например, для его проверки с помощью обновленных баз.

**РЕЗЕРВНОЕ ХРАНИЛИЩЕ**

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их первым лечением или удалением.

**РЕКОМЕНДУЕМЫЙ УРОВЕНЬ**

Уровень безопасности, базирующийся на параметрах работы программы, рекомендуемых экспертами «Лаборатории Касперского» и обеспечивающих оптимальную защиту вашего компьютера. Данный уровень установлен для использования по умолчанию.

**С****СЕРВЕРЫ ОБНОВЛЕНИЙ «ЛАБОРАТОРИИ КАСПЕРСКОГО»**

Список HTTP- и FTP-серверов «Лаборатории Касперского», с которых программа копирует базы и обновления модулей на ваш компьютер.

**СРОК ДЕЙСТВИЯ ЛИЦЕНЗИИ**

Период, в течение которого вам предоставляется возможность использовать полную функциональность программы «Лаборатории Касперского». Срок действия лицензии, как правило, составляет календарный год со дня ее установки. После окончания срока действия лицензии функциональность программы сокращается: вы не сможете обновлять базы программы.

**СРОЧНОЕ ОБНОВЛЕНИЕ**

Критическое обновление модулей программы «Лаборатории Касперского».

**СТАТУС ЗАЩИТЫ**

Текущее состояние защиты, характеризующее степень защищенности компьютера.

## Т

### ТЕХНОЛОГИЯ iСНЕСКЕР

Технология, позволяющая увеличить скорость антивирусной проверки за счет исключения тех объектов, которые не были изменены с момента предыдущей проверки, при условии, что параметры проверки (антивирусные базы и настройки) не были изменены. Информация об этом хранится в специальной базе. Технология применяется как в режиме постоянной защиты, так и в режиме проверки по требованию.

Например, у вас есть файл архива, который был проверен программой «Лаборатории Касперского» и ему был присвоен статус *незаражен*. В следующий раз этот архив будет исключен из проверки, если он не был изменен и не менялись параметры проверки. Если вы изменили состав архива, добавив в него новый объект, изменили параметры проверки, обновили антивирусные базы, архив будет проверен повторно.

Ограничения технологии iChecker:

- технология не работает с файлами больших размеров, так как в этом случае проверить весь файл быстрее, чем вычислять был ли он изменен с момента последней проверки;
- технология поддерживает ограниченное число форматов (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

## У

### УДАЛЕНИЕ ОБЪЕКТА

Способ обработки объекта, при котором происходит его физическое удаление с того места, где он был обнаружен программой (жесткий диск, папка, сетевой ресурс). Такой способ обработки рекомендуется применять к опасным объектам, лечение которых по тем или иным причинам невозможно.

### УДАЛЕНИЕ СООБЩЕНИЯ

Способ обработки электронного сообщения, содержащего признаки спама, при котором происходит его физическое удаление. Такой способ рекомендуется применять к сообщениям, однозначно содержащим спам. Перед удалением сообщения его копия сохраняется в резервном хранилище (если данная функциональность не отключен).

### УПАКОВАННЫЙ ФАЙЛ

Файл архива, который содержит в себе некоторую программу-распаковщик и инструкции операционной системе для ее выполнения.

### УРОВЕНЬ ВАЖНОСТИ СОБЫТИЯ

Характеристика события, зафиксированного в работе программы «Лаборатории Касперского». Существуют четыре уровня важности:

- **Критическое событие.**
- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

## Ф

### ФАЙЛ КЛЮЧА

Файл с расширением .key, который является вашим личным «ключом», необходимым для работы с программой «Лаборатории Касперского». Файл ключа входит в комплект поставки продукта, если вы приобрели его у дистрибьюторов «Лаборатории Касперского», или присылается вам по почте, если продукт был приобретен в интернет-магазине.

**Х****ХРАНИЛИЩЕ РЕЗЕРВНЫХ КОПИЙ**

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

**Э****ЭВРИСТИЧЕСКИЙ АНАЛИЗАТОР**

Технология обнаружения угроз, неопределяемых с помощью баз Антивируса. Позволяет находить объекты, которые подозреваются на заражение неизвестным вирусом или новой модификацией известного.

С помощью эвристического анализатора обнаруживаются до 92% новых угроз. Этот механизм достаточно эффективен и очень редко приводит к ложным срабатываниям.

Файлы, обнаруженные с помощью эвристического анализатора, признаются подозрительными.

# ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» была основана в 1997 году. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

«Лаборатория Касперского» – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

«Лаборатория Касперского» сегодня – это более тысячи высококвалифицированных специалистов, десять из которых имеют дипломы MBA, шестнадцать – степени кандидатов наук. Ведущие вирусные аналитики «Лаборатории Касперского» являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками в течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг «Лаборатории Касперского». Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. «Лаборатория Касперского» первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие мировые разработчики используют в своих продуктах программное ядро Антивируса Касперского, например, такие как: Nokia ICG (США), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты «Лаборатории Касперского» обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей технической поддержкой на нескольких языках.

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО «Лаборатория Касперского». Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Веб-сайт «Лаборатории Касперского»: <http://www.kaspersky.ru>

Вирусная энциклопедия: <http://www.viruslist.ru>

Антивирусная лаборатория: [newvirus@kaspersky.com](mailto:newvirus@kaspersky.com)

(только для отправки подозрительных объектов в архивированном виде)

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

(для запросов вирусным аналитикам)

# ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

## I

iSwift-файлы ..... 86

## A

Алгоритм работы  
Файловый Антивирус ..... 41

## B

Восстановление параметров по умолчанию ..... 48

## Г

Главное окно программы ..... 37

## Д

Действия над объектами ..... 42

Диск аварийного восстановления ..... 94, 96

ДИСК АВАРИЙНОГО ВОССТАНОВЛЕНИЯ ..... 93

Доверенная зона  
доверенные программы ..... 78, 81  
правила исключений ..... 78

## З

Запуск задачи  
обновление ..... 64, 67, 68  
проверка ..... 51, 59, 60

Зараженный объект ..... 158

Значок в области уведомлений панели задач ..... 35

## И

ИНТЕРФЕЙС ПРОГРАММЫ ..... 35

## К

Карантин ..... 91, 92

Карантин и резервное хранилище ..... 91, 92

Категории обнаруживаемых угроз ..... 77

Контекстное меню ..... 36

## Л

Лицензия ..... 162  
активная ..... 157  
получение файла ключа ..... 162

## О

Область защиты  
Файловый Антивирус ..... 44

Обновление  
вручную ..... 64  
из локальной папки ..... 69  
использование прокси-сервера ..... 66  
источник обновлений ..... 65  
откат последнего обновления ..... 65

по расписанию.....	68
предмет обновления.....	68
региональные настройки.....	66
режим запуска.....	67, 68
Ограничение доступа к программе.....	86
Отчеты.....	90

## П

Проверка	
автоматический запуск пропущенной задачи.....	58, 59
действие над обнаруженным объектом.....	54
оптимизация проверки.....	55
по расписанию.....	59
приостановка задачи.....	58, 59
проверка составных файлов.....	56
режим запуска.....	59
технологии проверки.....	57
тип проверяемых объектов.....	55
уровень безопасности.....	53

## Р

Реакция на угрозу	
проверка на вирусы.....	54
Файловый Антивирус.....	42
Резервное копирование.....	161
Резервное хранилище.....	92

## С

Самозащита программы.....	85
Статистика работы компонента	
Файловый Антивирус.....	48

## У

Уведомления.....	87
Уровень безопасности	
Файловый Антивирус.....	42

## Ф

Файловый Антивирус	
алгоритм работы.....	41
область защиты.....	44
оптимизация проверки.....	45
приостановка работы.....	47, 48
проверка составных файлов.....	45, 46
реакция на угрозу.....	42
режим проверки.....	46
статистика работы компонента.....	48
технология проверки.....	47
уровень безопасности.....	42
эвристический анализ.....	45

## Х

Хранилища	
резервное хранилище.....	163

## Э

Эвристический анализ	
Файловый Антивирус.....	45