

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского 7.0

РУКОВОДСТВО
ПОЛЬЗОВАТЕЛЯ

АНТИВИРУС КАСПЕРСКОГО 7.0

Руководство пользователя

© ЗАО «Лаборатория Касперского»
Тел., факс: +7 (495) 797-87-00, +7 (495) 645-79-39
<http://www.kaspersky.ru>

Дата редакции: май 2007 года

Содержание

ГЛАВА 1. УГРОЗЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ.....	9
1.1. Источники угроз	9
1.2. Распространение угроз.....	10
1.3. Виды угроз	12
1.4. Признаки заражения	16
1.5. Что делать при наличии признаков заражения.....	17
1.6. Профилактика заражения	18
ГЛАВА 2. АНТИВИРУС КАСПЕРСКОГО 7.0.....	21
2.1. Что нового в Антивирусе Касперского 7.0.....	21
2.2. На чем строится защита Антивируса Касперского	24
2.2.1. Компоненты постоянной защиты.....	24
2.2.2. Задачи поиска вирусов	26
2.2.3. Обновление	26
2.2.4. Сервисные функции приложения.....	27
2.3. Аппаратные и программные требования к системе	28
2.4. Комплект поставки.....	29
2.5. Сервис для зарегистрированных пользователей	30
ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО 7.0	31
3.1. Процедура установки с помощью мастера установки	31
3.2. Мастер первоначальной настройки.....	35
3.2.1. Использование объектов, сохраненных с версии 5.0.....	36
3.2.2. Активация приложения	36
3.2.2.1. Выбор способа активации приложения	37
3.2.2.2. Ввод кода активации	37
3.2.2.3. Регистрация пользователя.....	38
3.2.2.4. Получение файла ключа.....	38
3.2.2.5. Выбор файла ключа	38
3.2.2.6. Завершение активации приложения.....	39
3.2.3. Выбор режима защиты	39
3.2.4. Настройка параметров обновления.....	40

3.2.5. Настройка расписания проверки на вирусы	40
3.2.6. Ограничение доступа к приложению	41
3.2.7. Контроль целостности приложений	42
3.2.8. Завершение работы мастера настройки	42
3.3. Процедура установки приложения из командной строки	43
ГЛАВА 4. ИНТЕРФЕЙС ПРИЛОЖЕНИЯ	44
4.1. Значок в системной панели	44
4.2. Контекстное меню	45
4.3. Главное окно приложения	47
4.4. Окно настройки параметров приложения	50
ГЛАВА 5. НАЧАЛО РАБОТЫ	52
5.1. Каков статус защиты компьютера	52
5.2. Каков статус отдельного компонента защиты о	54
5.3. Как проверить на вирусы компьютер	55
5.4. Как проверить критические области компьютера	56
5.5. Как проверить на вирусы файл, каталог или диск	57
5.6. Как обновить приложение	57
5.7. Что делать, если защита не работает	58
ГЛАВА 6. КОМПЛЕКСНОЕ УПРАВЛЕНИЕ ЗАЩИТОЙ	59
6.1. Отключение / включение постоянной защиты вашего компьютера	59
6.1.1. Приостановка защиты	60
6.1.2. Полное отключение защиты компьютера	61
6.1.3. Приостановка / выключение отдельных компонентов защиты	62
6.1.4. Возобновление защиты вашего компьютера	63
6.2. Технология лечения активного заражения	63
6.3. Работа приложения на портативном компьютере	64
6.4. Производительность компьютера при выполнении задач	64
6.5. Решение проблем совместимости Антивируса Касперского с другими приложениями	65
6.6. Запуск задач поиска вирусов и обновления с правами другого пользователя	65
6.7. Настройка расписания запуска задач и отправки уведомлений	67
6.8. Типы контролируемых вредоносных программ	69
6.9. Формирование доверенной зоны	70
6.9.1. Правила исключений	71
6.9.2. Доверенные приложения	76

ГЛАВА 7. АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВОЙ СИСТЕМЫ КОМПЬЮТЕРА	80
7.1. Выбор уровня безопасности файлов	81
7.2. Настройка защиты файлов	83
7.2.1. Определение типов проверяемых файлов	83
7.2.2. Формирование области защиты	86
7.2.3. Настройка дополнительных параметров	88
7.2.4. Использование методов эвристического анализа	90
7.2.5. Восстановление параметров защиты файлов по умолчанию	92
7.2.6. Выбор действия над объектами	93
7.3. Отложенное лечение объектов	95
ГЛАВА 8. АНТИВИРУСНАЯ ЗАЩИТА ПОЧТЫ	96
8.1. Выбор уровня безопасности почты	97
8.2. Настройка защиты почты	99
8.2.1. Выбор защищаемого потока сообщений	100
8.2.2. Настройка проверки почты в Microsoft Office Outlook	102
8.2.3. Настройка проверки почты в The Bat!	103
8.2.4. Использование методов эвристического анализа	105
8.2.5. Восстановление параметров защиты почты по умолчанию	106
8.2.6. Выбор действия над опасным объектом письма	106
ГЛАВА 9. ВЕБ-ЗАЩИТА	109
9.1. Выбор уровня безопасности веб-защиты	110
9.2. Настройка веб-защиты	112
9.2.1. Определение алгоритма проверки	113
9.2.2. Формирование списка доверенных адресов	114
9.2.3. Использование методов эвристического анализа	115
9.2.4. Восстановление параметров веб-защиты по умолчанию	116
9.2.5. Выбор действия над опасным объектом	117
ГЛАВА 10. ПРОАКТИВНАЯ ЗАЩИТА ВАШЕГО КОМПЬЮТЕРА	119
10.1. Правила контроля активности	123
10.2. Контроль целостности приложений	127
10.2.1. Настройка правил контроля критических приложений	128
10.2.2. Формирование списка общих компонентов	130
10.3. Контроль изменений системного реестра	131
10.3.1. Выбор объектов реестра для создания правила	133

10.3.2. Создание правила для контроля ключей реестра	134
ГЛАВА 11. ПОИСК ВИРУСОВ НА КОМПЬЮТЕРЕ	136
11.1. Управление задачами поиска вирусов	137
11.2. Формирование списка объектов проверки.....	138
11.3. Создание задач поиска вирусов	139
11.4. Настройка задач поиска вирусов	140
11.4.1. Выбор уровня безопасности	141
11.4.2. Определение типов проверяемых объектов	142
11.4.3. Дополнительные параметры поиска вирусов.....	146
11.4.4. Поиск руткитов	147
11.4.5. Использование методов эвристического анализа	148
11.4.6. Восстановление параметров проверки по умолчанию	149
11.4.7. Выбор действия над объектами	149
11.4.8. Назначение единых параметров проверки для всех задач.....	152
ГЛАВА 12. ТЕСТИРОВАНИЕ РАБОТЫ АНТИВИРУСА КАСПЕРСКОГО	153
12.1. Тестовый «вирус» EICAR и его модификации	153
12.2. Проверка Файлового Антивируса.....	155
12.3. Проверка задачи Поиска вирусов	156
ГЛАВА 13. ОБНОВЛЕНИЕ ПРИЛОЖЕНИЯ	158
13.1. Запуск обновления.....	160
13.2. Откат последнего обновления.....	160
13.3. Настройка обновления	161
13.3.1. Выбор источника обновлений.....	161
13.3.2. Выбор режима и предмета обновления.....	164
13.3.3. Копирование обновлений.....	165
13.3.4. Действия после обновления приложения.....	166
ГЛАВА 14. УПРАВЛЕНИЕ КЛЮЧАМИ	168
ГЛАВА 15. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ.....	170
15.1. Карантин возможно зараженных объектов.....	171
15.1.1. Действия с объектами на карантине.....	172
15.1.2. Настройка параметров карантина.....	174
15.2. Резервные копии опасных объектов	175
15.2.1. Действия с резервными копиями	175
15.2.2. Настройка параметров резервного хранилища	177

15.3. Отчеты	177
15.3.1. Настройка параметров отчетов	180
15.3.2. Закладка <i>Обнаружено</i>	181
15.3.3. Закладка <i>События</i>	182
15.3.4. Закладка <i>Статистика</i>	183
15.3.5. Закладка <i>Параметры</i>	183
15.3.6. Закладка <i>Реестр</i>	185
15.4. Диск аварийного восстановления	185
15.4.1. Создание диска аварийного восстановления	186
15.4.2. Использование диска аварийного восстановления	188
15.5. Формирование списка контролируемых портов	189
15.6. Проверка защищенных соединений	191
15.7. Настройка параметров прокси-сервера	193
15.8. Настройка интерфейса Антивируса Касперского	195
15.9. Использование дополнительных сервисов	197
15.9.1. Уведомления о событиях Антивируса Касперского	198
15.9.1.1. Типы событий и способы отправки уведомлений	199
15.9.1.2. Настройка отправки уведомлений по электронной почте	201
15.9.1.3. Настройка параметров журнала событий	202
15.9.2. Самозащита приложения и ограничение доступа к ней	203
15.9.3. Экспорт / импорт параметров работы Антивируса Касперского	204
15.9.4. Восстановление параметров по умолчанию	205
15.10. Техническая поддержка пользователей	206
15.11. Завершение работы с приложением	208
ГЛАВА 16. РАБОТА С ПРИЛОЖЕНИЕМ ИЗ КОМАНДНОЙ СТРОКИ	210
16.1. Активация приложения	212
16.2. Управление компонентами приложения и задачами	212
16.3. Антивирусная проверка объектов	215
16.4. Обновление приложения	220
16.5. Откат последнего обновления приложения	221
16.6. Экспорт параметров защиты	222
16.7. Импорт параметров защиты	223
16.8. Запуск приложения	223
16.9. Остановка приложения	223
16.10. Получение файла трассировки	224
16.11. Просмотр справки	225

16.12. Коды возврата командной строки	225
ГЛАВА 17. ИЗМЕНЕНИЕ, ВОССТАНОВЛЕНИЕ ИЛИ УДАЛЕНИЕ ПРИЛОЖЕНИЯ	226
17.1. Изменение, восстановление и удаление приложения с помощью мастера установки	226
17.2. Удаление приложения из командной строки	228
ГЛАВА 18. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ	230
ПРИЛОЖЕНИЕ А. СПРАВОЧНАЯ ИНФОРМАЦИЯ	232
А.1. Список объектов, проверяемых по расширению	232
А.2. Разрешенные маски исключений файлов	234
А.3. Разрешенные маски исключений по классификации Вирусной энциклопедии	235
ПРИЛОЖЕНИЕ В. ООО «КРИПТОЭКС»	237
ПРИЛОЖЕНИЕ С. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»	238
С.1. Другие разработки «Лаборатории Касперского»	239
С.2. Наши координаты	250

ГЛАВА 1. УГРОЗЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

В связи со стремительным развитием информационных технологий и их проникновением во все сферы человеческой деятельности возросло количество преступлений, направленных против информационной безопасности.

Большой интерес со стороны кибер-преступников вызывает деятельность государственных структур и коммерческих предприятий. Целью является хищение, разглашение конфиденциальной информации, подрыв деловой репутации, нарушение работоспособности и, как следствие, доступности информационных ресурсов организации. Данные действия наносят огромный моральный и материальный ущерб.

Однако риску подвергаются не только крупные компании, но и частные пользователи. С помощью различных средств преступники получают доступ к персональным данным – номерам банковских счетов, кредитных карт, паролям, выводят систему из строя или получают полный доступ к компьютеру. В дальнейшем такой компьютер может использоваться как часть зомби-сети – сети зараженных компьютеров, использующихся злоумышленниками для проведения атак на серверы, рассылки спама, сбора конфиденциальной информации, распространения новых вирусов и троянских программ.

Сегодня всеми признается, что информация является ценным достоянием и подлежит защите. В то же время информация должна быть доступной для определенного круга пользователей (например, сотрудникам, клиентам и партнерам предприятия). Таким образом, встает вопрос о создании комплексной системы информационной безопасности. Такая система должна учитывать все возможные источники угроз (человеческий, технический и стихийный факторы) и использовать весь комплекс защитных мер, таких как физические, административные и программно-технические средства защиты.

1.1. Источники угроз

В качестве источника угроз информационной безопасности может выступать человек либо группа людей, а также некие, независящие от деятельности человека, проявления. Исходя из этого, все источники угроз можно разделить на три группы:

- **Человеческий фактор.** Данная группа угроз связана с действиями человека, имеющего санкционированный или несанкционированный доступ к информации. Угрозы этой группы можно разделить на:
 - внешние, к ним относятся действия кибер-преступников, хакеров, интернет-мошенников, недобросовестных партнеров, криминальных структур.
 - внутренние, к ним относятся действия персонала компаний, а также пользователей домашних компьютеров. Действия данных людей могут быть как умышленными, так и случайными.
- **Технический фактор.** Эта группа угроз связана с техническими проблемами – физическое и моральное устаревание используемого оборудования, некачественные программные и аппаратные средства обработки информации. Все это приводит к отказу оборудования и зачастую потери информации.
- **Стихийный фактор.** Эта группа угроз включает в себя природные катаклизмы, стихийные бедствия и прочие форс-мажорные обстоятельства, независящие от деятельности людей.

Все три источника угроз необходимо обязательно учитывать при разработке системы защиты информационной безопасности. В данном руководстве мы остановимся только на одном из них, непосредственно связанном с деятельностью компании «Лаборатория Касперского», – внешних угрозах, связанных с деятельностью человека.

1.2. Распространение угроз

Развитие современных компьютерных технологий и средств связи дает возможность злоумышленникам использовать различные источники распространения угроз. Рассмотрим их подробнее:

Интернет

Глобальная сеть Интернет уникальна тем, что не является чьей-то собственностью и не имеет территориальных границ. Это во многом способствует развитию многочисленных веб-ресурсов и обмену информацией. Сейчас любой человек может получить доступ к данным, хранящимся в интернете, или создать свой собственный веб-ресурс.

Однако эти же особенности глобальной сети предоставляют злоумышленникам возможность совершения преступлений в интернете, затрудняя их обнаружение и наказание.

Злоумышленники размещают вирусы и другие вредоносные программы на веб-ресурсах, «маскируют» их под полезное и бесплатное программное обеспечение. Кроме того, скрипты, автоматически за-

пускаемые при открытии некоторых веб-страниц, могут выполнять вредоносные действия на вашем компьютере, включая изменение системного реестра, кражу личных данных и установку вредоносного программного обеспечения.

Используя сетевые технологии, злоумышленники реализуют атаки на удаленные частные компьютеры и серверы компаний. Результатом таких атак может являться выведение ресурса из строя, получение полного доступа к ресурсу, а, следовательно, к информации, хранящейся на нем, использование ресурса как части зомби-сети.

В связи с появлением кредитных карт, электронных денег и возможностью их использования через интернет (интернет-магазины, аукционы, персональные страницы банков и т.д.) интернет-мошенничество стало одним из наиболее распространенных преступлений.

Интранет

Интранет – это внутренняя сеть, специально разработанная для управления информацией внутри компании или, например, частной домашней сети. Интранет является единым пространством для хранения, обмена и доступа к информации для всех компьютеров сети. Поэтому, если какой-либо из компьютеров сети заражен, остальные компьютеры подвергаются значительному риску заражения. Во избежание возникновения таких ситуаций необходимо защищать не только периметр сети, но и каждый отдельный компьютер.

Электронная почта

Наличие почтовых приложений практически на каждом компьютере, а также то, что вредоносные программы полностью используют содержимое электронных адресных книг для выявления новых жертв, обеспечивает благоприятные условия для распространения вредоносных программ. Пользователь зараженного компьютера, сам того не подозревая, рассылает зараженные письма адресатам, которые, в свою очередь, отправляют новые зараженные письма и т.д. Нередки случаи, когда зараженный файл-документ по причине недосмотра попадает в списки рассылки коммерческой информации какой-либо крупной компании. В этом случае страдают не пять, а сотни или даже тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысяч своих абонентов.

Помимо угрозы проникновения вредоносных программ существуют проблема внешней нежелательной почты рекламного характера (спама). Не являясь источником прямой угрозы, нежелательная корреспонденция увеличивает нагрузку на почтовые серверы, создает дополнительный трафик, засоряет почтовый ящик пользователя, ведет к потере рабочего времени и тем самым наносит значительный финансовый урон.

Также важно отметить, что злоумышленники стали использовать так называемые спамерские технологии массового распространения и методы социального инжиниринга, чтобы заставить пользователя открыть письмо, перейти по ссылке из письма на некий интернет-ресурс и т.п. Из этого следует, что возможности фильтрации спама важны не только сами по себе, но и для противодействия некоторым новым видам интернет-мошенничества (например, фишингу), а также распространению вредоносных программ.

Съемные носители информации

Съемные носители – дискеты, CD/DVD-диски, флеш-карты – широко используются для хранения и передачи информации.

При запуске файла, содержащего вредоносный код, со съемного носителя вы можете повредить данные, хранящиеся на вашем компьютере, а также распространить вирус на другие диски компьютера или компьютеры сети.

1.3. Виды угроз

В настоящее время существует огромное количество угроз, которым может подвергнуться ваш компьютер. В данном разделе мы подробнее остановимся на угрозах, блокируемых Антивирусом Касперского:

Черви (Worms)

Данная категория вредоносных программ для распространения использует в основном уязвимости операционных систем. Название этого класса было дано исходя из способности червей «переползать» с компьютера на компьютер, используя сети и электронную почту. Также благодаря этому многие черви обладают достаточно высокой скоростью распространения.

Черви проникают на компьютер, осуществляют поиск сетевых адресов других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Вирусы (Viruses)

Программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – *заражение*.

Троянские программы (Trojans)

Программы, которые выполняют на поражаемых компьютерах не-санкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к «зависанию», воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

В последнее время наиболее распространенными типами вредоносных программ, портящими компьютерные данные, стали черви. Далее по распространенности следуют вирусы и троянские программы. Некоторые вредоносные программы совмещают в себе характеристики двух или даже трех из перечисленных выше классов.

Программы-рекламы (Adware)

Программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе, изменяют различные параметры браузера (стартовые и поисковые страницы, уровни безопасности и т.д.), а также создают неконтролируемый пользователем трафик. Все это может привести как к нарушению политики безопасности, так и к прямым финансовым потерям.

Программы-шпионы (Spyware)

Программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере вы можете и не догадываться. Как правило, целью программ-шпионов является:

- отслеживание действий пользователя на компьютере;
- сбор информации о содержании жесткого диска; в этом случае чаще всего речь идет о сканировании некоторых каталогов и системного реестра с целью составления списка программного обеспечения, установленного на компьютере;
- сбор информации о качестве связи, способе подключения, скорости модема и т.д.

Потенциально опасные приложения (Riskware)

К потенциально опасным относятся приложения, которые не имеют вредоносных функций, но могут являться частью среды разработки вредоносного программного обеспечения или использоваться злоумышленниками в качестве вспомогательных компонентов вредоносных программ. К категории таких программ относятся программы, имеющие бреши и ошибки, а также некоторые утилиты удаленного администрирования, программы автоматического переключения раскладки клавиатуры, IRC-клиенты, FTP-серверы, всевозможные утилиты для остановки процессов или скрытия их работы.

Еще одним видом вредоносных программ, являющимся пограничным для таких программ как Adware, Spyware и Riskware, являются программы, встраивающиеся в установленный на компьютере браузер и перенаправляющие трафик. Наверняка вы встречались с подобными программами, если при запросе одного адреса веб-сайта открывался совсем другой.

Программы-шутки (Jokes)

Программное обеспечение, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен либо будет причинен при каких-либо условиях. Такие программы часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

Руткиты (Rootkit)

Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Руткиты модифицируют операционную систему на компьютере и заменяют основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Прочие опасные программы

Программы, созданные для организации DoS-атак на удаленные серверы, взлома других компьютеров, а также являющиеся частью среды разработки вредоносного программного обеспечения. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов, сканеры уязвимостей, программы для взлома паролей, прочие виды программ для взлома сетевых ресурсов или проникновения в атакуемую систему.

Хакерские атаки

Хакерские атаки – это действия злоумышленников или вредоносных программ, направленные на захват информационных данных уда-

ленного компьютера, выведение системы из строя или получение полного контроля над ресурсами компьютера.

Некоторые виды интернет-мошенничества

Фишинг (Phishing) – вид интернет-мошенничества, заключающийся в рассылке электронных сообщений с целью кражи конфиденциальной информации, как правило, финансового характера. Фишинг-сообщения составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, специально подготовленный злоумышленниками и являющийся копией сайта организации, от имени которой пришло письмо. На данном сайте пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

Дозвон на платные интернет-ресурсы – вид интернет-мошенничества, связанный с несанкционированным использованием платных интернет-ресурсов (чаще всего это веб-сайты порнографического содержания). Установленные злоумышленниками программы (dialers) иницируют модемное соединение с вашего компьютера на платный номер. Чаще всего используемые номера имеют очень высокие тарифы, в результате пользователь вынужден оплачивать огромные телефонные счета.

Навязчивая реклама

Навязчивая реклама – это всплывающие окна и рекламные баннеры, открывающиеся при работе с веб-сайтами. Как правило, информация, содержащаяся в них, не бывает полезной. Демонстрация всплывающих окон и баннеров отвлекает пользователя от основных задач, увеличивает объем трафика.

Спам (Spam)

Спам – это анонимная массовая рассылка нежелательных почтовых сообщений. Так, спамом являются рассылки рекламного, политического и агитационного характера, письма, призывающие помочь кому-нибудь. Отдельную категорию спама составляют письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды, а также письма, направленные на кражу паролей и номеров кредитных карт, письма с просьбой переслать знакомым (например, письма счастья) и т. п. Спам существенно увеличивает нагрузку на почтовые серверы и повышает риск потери информации, важной для пользователя.

Обнаружение и блокирование данных видов угроз Антивирусом Касперского осуществляется с помощью двух методов:

- *реактивный* – метод, основанный на поиске вредоносных объектов с помощью постоянно обновляемых баз приложения. Для реализации

данного метода необходимо хотя бы одно заражение, чтобы добавить сигнатуру угрозы в базы и распространить обновление баз.

- *проактивный* – метод, в отличие от реактивной защиты, строящийся не на анализе кода объекта, а на анализе его поведения в системе. Этот метод нацелен на обнаружение новых угроз, информации о которых еще нет в базах.

Применение обоих методов в Антивирусе Касперского обеспечивает комплексную защиту вашего компьютера от известных, а также новых угроз.

Внимание!

Далее по тексту Руководства в качестве обозначения вредоносных и опасных программ мы будем использовать термин «вирус». Акцент на конкретный вид вредоносной программы будет делаться только в случае, когда это необходимо.

1.4. Признаки заражения

Есть ряд признаков, свидетельствующих о заражении компьютера. Если вы замечаете, что с компьютером происходят «странные» вещи, а именно:

- на экран выводятся непредусмотренные сообщения, изображения либо воспроизводятся непредусмотренные звуковые сигналы;
- неожиданно открывается и закрывается лоток CD/DVD-ROM-устройства;
- произвольно, без вашего участия, на вашем компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя вы никак не инициировали такое ее поведение, то, с большой степенью вероятности, можно предположить, что ваш компьютер поражен вирусом.

Кроме того, есть некоторые характерные признаки поражения вирусом через почту:

- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера.

Есть также косвенные признаки заражения вашего компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- веб-браузер (например, Microsoft Internet Explorer) «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуется провести полную проверку вашего компьютера (см. п. 5.3 на стр. 55).

1.5. Что делать при наличии признаков заражения

Если вы заметили, что ваш компьютер «ведет себя подозрительно»,

1. Не паникуйте! Не поддаваться панике – золотое правило, которое может избавить вас от потери важных данных.
2. Отключите компьютер от интернета и локальной сети, если он к ней был подключен.
3. Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Microsoft Windows, который вы создавали при установке операционной системы на компьютер.
4. Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (дискету, CD/DVD-диск, флеш-карту и пр.).
5. Установите Антивирус Касперского, если вы этого еще не сделали.
6. Обновите базы и модули приложения (см. п. 5.6 на стр. 57). Если это возможно, для их получения выходите в интернет не со своего компьютера, а с незараженного компьютера друзей, интернет-кафе, с работы. Лучше воспользоваться другим компьютером, по-

сколько при подключении к интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги. Именно поэтому при подозрении на заражение лучше всего сразу отключиться от интернета. Вы также можете получить обновления баз на дискете или диске у «Лаборатории Касперского» или ее дистрибьюторов и обновить свои базы с этого источника.

7. Установите рекомендуемый экспертами «Лаборатории Касперского» уровень защиты.
8. Запустите полную проверку компьютера (см. п. 5.3 на стр. 55).

1.6. Профилактика заражения

Никакие самые надежные и разумные меры не смогут обеспечить стопроцентную защиту от компьютерных вирусов и троянских программ, но, выработав для себя ряд правил, вы существенно снизите вероятность вирусной атаки и степень возможного ущерба.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная *профилактика*. Компьютерная профилактика состоит из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и потери каких-либо данных.

Ниже перечислены основные правила безопасности, выполнение которых позволит вам избежать риска вирусных атак.

Правило № 1: защитите ваш компьютер с помощью антивирусных программ и программ безопасной работы в интернете. Для этого:

- Безотлагательно установите Антивирус Касперского.
- Регулярно обновляйте базы, входящие в состав приложения (см. п. 5.6 на стр. 57). Обновление можно проводить несколько раз в день при возникновении вирусных эпидемий – в таких ситуациях базы приложения на серверах обновлений «Лаборатории Касперского» обновляются немедленно.
- Задайте рекомендуемые экспертами «Лаборатории Касперского» параметры защиты вашего компьютера. Защита начинает действовать сразу после включения компьютера и затрудняет вирусам проникновение на компьютер.
- Задайте рекомендуемые экспертами «Лаборатории Касперского» параметры для полной проверки компьютера и запланируйте ее выполнение не реже одного раза в неделю.

Правило № 2: будьте осторожны при записи новых данных на компьютер:

- Проверяйте на присутствие вирусов все съемные диски (дискеты, CD/DVD-диски, флеш-карты и пр.) перед их использованием (см. п. 5.5 на стр. 57).
- Осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам, даже если они отправлены вашими знакомыми.
- Внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта вам предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.
- Если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его с помощью Антивируса Касперского.
- Внимательно относитесь к выбору посещаемых вами интернет-ресурсов. Некоторые из сайтов заражены опасными скрипт-вирусами или интернет-червями.

Правило № 3: внимательно относитесь к информации от «Лаборатории Касперского».

В большинстве случаев «Лаборатория Касперского» сообщает о начале новой эпидемии задолго до того, как она достигнет своего пика. Вероятность заражения в этом случае еще невелика, и, скачав обновленные базы приложения, вы сможете защитить себя от нового вируса заблаговременно.

Правило № 4: с недоверием относитесь к вирусным мистификациям – программам-шуткам, письмам об угрозах заражения.

Правило № 5: пользуйтесь сервисом *Windows Update* и регулярно устанавливайте обновления операционной системы Microsoft Windows.

Правило № 6: покупайте дистрибутивные копии программного обеспечения у официальных продавцов.

Правило № 7: ограничьте круг людей, допущенных к работе на вашем компьютере.

Правило № 8: уменьшите риск неприятных последствий возможного заражения:

- Своевременно делайте резервное копирование данных. В случае потери данных система достаточно быстро может быть восстановлена при наличии резервных копий. Дистрибутивные диски, дискеты, флеш-карты и другие носители с программным обеспечением и ценной информацией должны храниться в надежном месте.

- Обязательно создайте диск аварийного восстановления (см. п. 15.4 на стр. 185), с которого при необходимости можно будет загрузиться, используя «чистую» операционную систему.

Правило № 9: *регулярно просматривайте список установленных на вашем компьютере программ.* Для этого вы можете воспользоваться сервисом **Установка / удаление программ** в **Панели инструментов** или просто просмотреть содержимое каталога **Program Files**, каталога автозагрузки. Таким образом, вы можете обнаружить программное обеспечение, которое было установлено на компьютер без вашего ведома, пока вы, например, пользовались интернетом или устанавливали некоторую программу. Наверняка некоторые из них могут оказаться потенциально опасными программами.

ГЛАВА 2. АНТИВИРУС КАСПЕРСКОГО 7.0

Антивирус Касперского 7.0 – это новое поколение решений по защите информации.

Основное отличие Антивируса Касперского 7.0 от существующих продуктов, в том числе и от продуктов компании ЗАО «Лаборатория Касперского», – это комплексный подход к защите информации на компьютере пользователя.

2.1. Что нового в Антивирусе Касперского 7.0

Антивирус Касперского 7.0 – это принципиально новый подход к защите информации. Главное в приложении – это объединение и заметное улучшение текущих функциональных возможностей всех продуктов компании в одно комплексное решение защиты. Приложение обеспечивает не только антивирусную защиту, но и защиту от неизвестных угроз.

Больше не нужно устанавливать несколько продуктов на компьютер, чтобы обеспечить себе полноценную защиту. Достаточно просто установить Антивирус Касперского 7.0.

Комплексная защита обеспечивается на всех каналах поступления и передачи информации. Гибкая настройка любого компонента приложения позволяет гибко адаптировать Антивирус Касперского под нужды конкретного пользователя. Предусмотрена также единая настройка всех компонентов защиты.

Рассмотрим детально нововведения Антивируса Касперского 7.0.

Новое в защите

- Теперь Антивирус Касперского защищает не только от уже известных вредоносных программ, но и от тех, что еще не известны. Наличие компонента проактивной защиты (см. Глава 10 на стр. 119) – основное преимущество приложения. Его работа построена на анализе поведения приложений, установленных на вашем компьютере, на контроле изменений системного реестра и борьбе со скрытыми угрозами. В работе компонента используется эвристический анализатор, позволяющий обнаруживать различные виды вредоносных программ. При этом ведется история вредоносной активности, на основе которой обеспечивается откат действий, совершенных вредоносной

программой, и восстановление системы до состояния, предшествующего вредоносному воздействию.

- Изменилась технология защиты файлов на компьютере пользователя: теперь вы можете снизить нагрузку на центральный процессор и дисковые подсистемы и увеличить скорость проверки файлов. Это достигается за счет использования технологий iChecker™ и iSwift™. Такой режим работы приложения исключает повторную проверку файлов.
- Процесс поиска вирусов теперь подстраивается под вашу работу на компьютере. Проверка может занимать достаточное количество времени и ресурсов системы, но пользователь может параллельно выполнять свою работу. Если выполнение какой-либо операции требует ресурсов системы, поиск вирусов будет приостановлен до момента завершения этой операции. Затем проверка продолжится с того места, на котором остановилась.
- Проверка критических областей компьютера, объектов автозапуска, заражение которых может привести к серьезным последствиям, а также обнаружение руткитов, скрывающих в системе вредоносные программы, представлены отдельными задачами. Вы можете настроить автоматический запуск этих задач каждый раз при старте системы.
- Значительно улучшена защита электронной корреспонденции на компьютере пользователя от вредоносных программ. Приложение проверяет на вирусы почтовый трафик на следующих протоколах:
 - IMAP, SMTP, POP3, независимо от используемого вами почтового клиента;
 - NNTP, независимо от почтового клиента;
 - независимо от типа протокола (в том числе MAPI, HTTP) в рамках работы плагинов, встроенных в почтовые программы Microsoft Office Outlook и The Bat!
- В таких широко известных почтовых клиентах как Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail) и The Bat! встроены специальные модули расширения (плагины), позволяющие настраивать защиту почты непосредственно в почтовом клиенте.
- Расширена функция оповещения пользователя (см. п. 15.9.1 на стр. 198) о возникновении в работе приложения определенных событий. Вы сами можете выбрать способ уведомления для каждого из типов событий: почтовое сообщение, звуковое оповещение, всплывающее сообщение, запись в журнал событий.
- Реализована проверка трафика, передаваемого через защищенное соединение по протоколу SSL.

- Добавлена технология самозащиты приложения, защиты от удаленного несанкционированного управления сервисом Антивируса, а также защиты доступа к параметрам приложения с помощью пароля. Это позволяет избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.
- Добавлена возможность создания диска аварийного восстановления системы. С помощью этого диска можно провести первоначальную загрузку операционной системы после вирусной атаки и выполнить проверку компьютера на наличие вредоносных объектов.
- Добавлен Новостной Агент – модуль, предназначенный для оперативной доставки новостей от «Лаборатории Касперского».

Новое в интерфейсе приложения

- В новом интерфейсе Антивируса Касперского реализован простой и удобный доступ к любой функции приложения. Вы также можете менять внешний вид приложения, используя свои графические элементы и цветовую палитру.
- При работе с приложением вы получаете полную информационную поддержку: Антивирус Касперского выводит информационные сообщения о состоянии защиты, включает подробную справку. Мастер безопасности, включенный в состав приложения, позволяет получить полную картину текущего состояния защиты компьютера и перейти к немедленному устранению проблем.

Новое в обновлении приложения

- В данной версии приложения реализована усовершенствованная процедура обновления: в автоматическом режиме Антивирус Касперского проверяет наличие пакета обновлений в источнике обновления. При обнаружении свежих обновлений приложение скачивает их и устанавливает на компьютер.
- С источника обновлений скачиваются только недостающие вам обновления. Это позволяет снизить объем скачиваемого при обновлении трафика до 10 раз.
- Обновление производится с наиболее эффективного источника.
- Теперь вы можете не использовать прокси-сервер, если обновление приложения выполняется из локального источника. Это заметно снижает объем трафика, проходящего через прокси-сервер.
- Реализована возможность отката обновлений, позволяющая в случае, например, повреждения файлов или ошибки копирования, вернуться к предыдущей версии баз приложения.

- Добавлена возможность использования сервиса копирования обновлений в локальный каталог для предоставления доступа к ним другим компьютерам сети с целью экономии интернет-трафика.

2.2. На чем строится защита Антивируса Касперского

Защита Антивируса Касперского строится исходя из источников угроз, то есть на каждый источник предусмотрен отдельный компонент приложения, обеспечивающий его контроль и необходимые мероприятия по предотвращению вредоносного воздействия этого источника на данные пользователя. Такое построение системы защиты позволяет гибко настраивать приложение под нужды конкретного пользователя или предприятия в целом.

Антивирус Касперского включает:

- Компоненты постоянной защиты (см. п. 2.2.1 на стр. 24), обеспечивающие защиту вашего компьютера на всех каналах поступления и передачи информации в режиме реального времени.
- Задачи поиска вирусов (см. п. 2.2.2 на стр. 26), посредством которых выполняется поиск вирусов в отдельных файлах, папках, дисках или областях, либо полная проверка компьютера.
- Обновление (см. 2.2.3 на стр. 26), обеспечивающее актуальность внутренних модулей приложения, а также баз, использующихся для поиска вредоносных программ.
- Сервисные функции (см. п. 2.2.3 на стр. 26), обеспечивающие информационную поддержку в работе с приложением и позволяющие расширить ее функциональность.

2.2.1. Компоненты постоянной защиты

Защита вашего компьютера в реальном времени обеспечивается следующими компонентами защиты:

Файловый Антивирус

Файловая система может содержать вирусы и прочие опасные программы. Вредоносные программы могут годами храниться в файловой системе компьютера, 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 вашем компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается приложением, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен Антивирусом. Если же файл по каким-либо причинам невозможно вылечить, он будет удален, при этом копия файла будет сохранена в резервном хранилище (см. п. 15.2 на стр. 175) или помещена на карантин (см. п. 15.1 на стр. 171).

Почтовый Антивирус

Электронная почтовая корреспонденция широко используется злоумышленниками для распространения вредоносных программ. Она является одним из основных средств распространения червей. Поэтому крайне важно контролировать все почтовые сообщения.

Почтовый Антивирус – компонент проверки всех входящих и исходящих почтовых сообщений вашего компьютера. Он анализирует электронные письма на присутствие вредоносных программ. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов.

Веб-Антивирус

Открывая в интернете различные веб-сайты, вы рискуете заразить компьютер вирусами, которые будут установлены на него при помощи скриптов, содержащихся на веб-страницах, а также загрузить опасный объект на свой компьютер.

Веб-Антивирус специально разработан для предотвращения подобных ситуаций. Данный компонент перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу. Строгому контролю также подвергается весь http-трафик.

Проактивная защита

С каждым днем вредоносных программ становится все больше, они усложняются, комбинируя в себе несколько видов, изменяются методы их распространения, они становятся все более сложными для обнаружения.

Для того чтобы обнаружить новую вредоносную программу еще до того, как она успеет нанести вред, «Лабораторией Касперского» разработан специальный компонент – *Проактивная защита*. Он основан на контроле и анализе поведения всех программ, установленных на вашем компьютере. На основании выполняемых действий Антивирус Касперского принимает решение: является программа потенциально опасной или нет. Таким образом, ваш компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных.

2.2.2. Задачи поиска вирусов

Помимо постоянной защиты всех источников проникновения вредоносных программ крайне важно периодически проводить проверку вашего компьютера на присутствие вирусов. Это необходимо делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами постоянной защиты из-за, например, установленного низкого уровня защиты или по другим причинам.

Для поиска вирусов в состав Антивируса Касперского включены следующие задачи:

Критические области

Проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты, исполняемые при старте системы, загрузочные секторы дисков, системные каталоги *Microsoft Windows*. Цель задачи – быстрое обнаружение в системе активных вирусов без запуска полной проверки компьютера.

Мой Компьютер

Поиск вирусов на вашем компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов.

Объекты автозапуска

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы, а также оперативной памяти и загрузочных секторов дисков.

Поиск руткитов (Rootkit)

Поиск на компьютере руткитов, обеспечивающих сокрытие вредоносных программ в операционной системе. Данные утилиты внедряются в систему, маскируя свое присутствие, а также наличие в системе процессов, каталогов, ключей реестра любых вредоносных программ, описанных в конфигурации руткита.

Также предусмотрена возможность создавать другие задачи поиска вирусов и формировать расписание их запуска. Например, можно создать задачу проверки почтовых баз раз в неделю или задачу поиска вирусов в каталоге **Мои документы**.

2.2.3. 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 приложения, используемых в работе Антивируса Касперского.

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

2.2.4. Сервисные функции приложения

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

Отчеты и файлы данных

В процессе работы приложения по каждому компоненту постоянной защиты, задаче поиска вирусов или обновлению приложения формируется отчет. Он содержит информацию о выполненных операциях и результаты работы. Пользуясь функцией *Отчеты*, 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 помочь вам как можно быстрее.

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 приложением 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.

Активация

При покупке Антивируса Касперского между вами и «Лабораторией Касперского» заключается лицензионное соглашение, на основе которого вы можете использовать приложение и получать доступ к обновлению баз приложения и Службе технической поддержки в течение

ние определенного временного периода. Срок использования, а также другая информация, необходимая для полнофункциональной работы приложения, указана в файле ключа.

Пользуясь функцией *Активация*, вы можете получить подробную информацию об используемом вами ключе, а также приобретении нового ключа.

Поддержка

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

С помощью соответствующих ссылок вы можете перейти на форум пользователей продуктов «Лаборатории Касперского», а также отправить в Службу технической поддержки сообщение об ошибке или отзыв о работе приложения, заполнив специальную форму на сайте.

Также для вас доступна Служба технической поддержки он-лайн, сервисы Персонального кабинета пользователя, и, конечно, наши сотрудники всегда готовы вам помочь в работе с Антивирусом Касперского по телефону.

2.3. Аппаратные и программные требования к системе

Для нормального функционирования Антивируса Касперского 7.0, компьютер должен удовлетворять следующим минимальным требованиям:

Общие требования:

- 50 МБ свободного места на жестком диске.
- CD-ROM (для установки Антивируса Касперского 7.0 с дистрибутивного CD-диска).
- Microsoft Internet Explorer 5.5 или выше (для обновления баз и модулей приложения через интернет).
- Microsoft Windows Installer 2.0.

Microsoft Windows 2000 Professional (Service Pack 4 или выше), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 2 или выше), Microsoft Windows XP Professional x64 Edition:

- Процессор Intel Pentium 300 МГц или выше (или совместимый аналог).
- 128 МБ свободной оперативной памяти.

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Процессор Intel Pentium 800 МГц 32-bit (x86)/ 64-bit (x64) или выше (или совместимый аналог).
- 512 MB свободной оперативной памяти.

2.4. Комплект поставки

Антивирус Касперского вы можете приобрести у наших дистрибьюторов (коробочный вариант), а также в одном из интернет-магазинов (например, www.kaspersky.ru, раздел **Электронный 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.
- Код активации приложения, наклеенный на конверт с установочным компакт-диском.
- Руководство пользователя.
- 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» (раздел **Загрузить → Дистрибутивы продуктов**). Руководство пользователя вы можете скачать из раздела **Загрузить → Документация**.

Код активации будет вам отправлен по электронной почте по факту оплаты.

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 дистрибьютору, 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.

2.5. Сервис для зарегистрированных пользователей

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

После активации приложения вы становитесь зарегистрированным пользователем приложения и в течение срока действия ключа можете получать следующие услуги:

- предоставление новых версий данного программного продукта;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного 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»).

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

ГЛАВА 3. УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО 7.0

Установка приложения может быть выполнена с помощью мастера установки (см. п. 3.1 на стр. 31) или из командной строки (см. п. 3.3 на стр. 43).

При установке с помощью мастера вы можете выбрать вариант быстрой установки. В данном случае не требуется активного участия пользователя в процессе установки: приложение будет установлено полностью с использованием параметров по умолчанию, рекомендуемых специалистами «Лаборатории Касперского». Однако в конце процедуры установки потребуется активировать приложение.

Вариант выборочной установки позволяет выбрать количество устанавливаемых компонентов защиты, каталог установки, а также провести активацию приложения и его первоначальную настройку с помощью специального мастера.

3.1. Процедура установки с помощью мастера установки

Перед началом установки Антивируса Касперского рекомендуется закрыть все работающие приложения.

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

Примечание.

Установка приложения с дистрибутива, полученного через интернет, полностью совпадает с установкой приложения 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 приложения на компьютер.

Рассмотрим подробно каждый шаг процедуры установки пакета.

Шаг 1. Проверка соответствия системы необходимым условиям установки Антивируса Касперского

Перед установкой приложения на вашем компьютере выполняется проверка соответствия установленных операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки Антивируса Касперского. Также проверяется наличие на вашем 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 ваш 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.

Шаг 4. Выбор типа установки

На данном этапе вам предлагается выбрать наиболее подходящий тип установки приложения:

Быстрая установка. При выборе данного варианта Антивирус Касперского будет полностью установлен на ваш компьютер с параметрами по умолчанию, рекомендуемыми специалистами «Лаборатории

Касперского». По окончании установки будет запущен мастер активации приложения (см. п. 3.2.2 на стр. 36).

Выборочная установка. В данном случае вам будет предложено выбрать, какие компоненты приложения вы хотите установить на ваш компьютер, указать каталог, куда будет установлено приложение, а также провести активацию приложения и его первоначальную настройку с помощью специального мастера (см. п. 3.2 на стр. 35).

При выборе первого варианта установка будет проведена без запроса каких-либо действий пользователя, то есть все последующие шаги, описанные в данном разделе, будут пропущены. Во втором случае на каждом этапе установки от вас потребуются ввод либо подтверждение некоторых данных.

Шаг 5. Выбор каталога установки

Следующий этап установки Антивируса Касперского определяет каталог на вашем компьютере, в который будет установлено приложение. По умолчанию задан путь: <Диск>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 7.0\.

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 вводите полное имя каталога установки вручную, оно не должно превышать 200 символов и содержать спецсимволы.

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

Шаг 6. Выбор компонентов приложения для установки

Данный шаг выполняется только в том случае, если вы выбрали **Выборочную** установку приложения на ваш компьютер.

При выборочной установке вам нужно определить список компонентов Антивируса Касперского, которые вы хотите установить. По умолчанию для установки выбраны все компоненты постоянной защиты и компонент поиска вирусов.

Для того чтобы выбрать компонент для последующей установки, нужно открыть контекстное меню по правой 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.

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 7. Поиск других антивирусных программ

На этом этапе осуществляется поиск других установленных на вашем компьютере 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 вашем компьютере их список будет выведен на экран. Вам будет предложено удалить их, прежде чем продолжить установку.

Под списком обнаруженных антивирусных приложений вы можете выбрать, автоматически удалить их или вручную.

Если в числе обнаруженных антивирусных программ есть Антивирус Касперского Personal или Антивирус Касперского Personal Pro, перед их удалением рекомендуем вам сохранить используемый в работе этих программ файл ключа. Вы сможете использовать его в качестве ключа для Антивируса Касперского 7.0. Также рекомендуем сохранить объекты карантина и резервного хранилища, эти объекты будут автоматически помещены в соответствующие хранилища Антивируса Касперского, и вы сможете продолжить работу с ними.

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

Шаг 8. Завершающая подготовка к установке приложения

На данном этапе вам будет предложено произвести завершающую подготовку к установке приложения на ваш компьютер. Вы можете определить, хотите ли вы использовать в работе приложения параметры защиты и базы приложения, если таковые были сохранены на вашем компьютере при удалении предыдущей версии Антивируса Касперского.

Рассмотрим подробнее, как включить использование описанных выше возможностей.

Если на вашем компьютере ранее была установлена предыдущая версия (сборка) Антивируса Касперского, и при ее удалении вы сохранили на компьютере базы приложения, вы можете подключить их для использования в устанавливаемой версии. Для этого установите флажок **Базы приложе-**

ния. Базы, включенные в поставку приложения, не будут копироваться на ваш компьютер.

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

При первоначальной установке Антивируса Касперского 7.0 не рекомендуется снимать флажок **Включить защиту модулей до начала установки**. Включенная защита модулей позволит, в случае возникновения ошибок в ходе установки приложения, провести корректную процедуру отката установки. При повторной попытке установки приложения рекомендуется снять данный флажок. Для продолжения установки нажмите на кнопку **Далее**.

При удаленной установке приложения на компьютер через **Windows Remote Desktop** рекомендуется снимать флажок **Включить защиту модулей до начала установки**. В противном случае процедура установки может быть не проведена или проведена некорректно.

Шаг 9. Завершение процедуры установки

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

Если для корректного завершения установки необходимо перезагрузить компьютер, на экран будет выведено соответствующее уведомление. После перезапуска системы автоматически будет запущен мастер первоначальной настройки Антивируса Касперского.

Если для завершения установки не требуется перезагружать систему, нажмите на кнопку **Далее**, чтобы перейти к мастеру первоначальной настройки приложения.

3.2. Мастер первоначальной настройки

Мастер настройки Антивируса Касперского 7.0 запускается в конце процедуры установки приложения. Его задача – помочь вам провести первичную настройку параметров приложения, 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 **Го-**

тово. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Вы можете пропустить этап первоначальной настройки при установке приложения, закрыв окно мастера. В дальнейшем его можно будет запустить из интерфейса приложения при восстановлении первоначальных параметров защиты Антивируса Касперского (см. п. 15.9.4 на стр. 205).

3.2.1. Использование объектов, сохраненных с версии 5.0

Данное окно мастера появляется при установке приложения поверх Антивируса Касперского версии 5.0. Вам предлагается выбрать, какие данные, используемые версией 5.0, требуется перенести в версию 7.0. Это могут быть объекты карантина, резервного хранилища либо параметры защиты.

Для того чтобы использовать эти данные в версии 7.0 установите необходимые флажки.

3.2.2. Активация приложения

Перед активацией приложения убедитесь, что параметры системной даты компьютера соответствуют реальной дате и времени.

Процедура активации приложения заключается в установке ключа, на основании которого Антивирус Касперского будет проверять наличие прав на использование приложения и определять срок его использования.

Ключ содержит служебную информацию, необходимую для полноценной работы приложения, а также дополнительные сведения:

- информация о поддержке (кто осуществляет и где можно ее получить);
- название и номер ключа, а также его окончания.

Внимание!

Для активации приложения требуется подключение к интернету. Если на момент установки соединение с интернетом отсутствует, вы можете провести активацию позже (см. п. Глава 14 на стр. 168) из интерфейса приложения либо, выйдя в интернет с другого компьютера, получить ключ по коду активации, зарегистрировавшись на веб-сайте Службы технической поддержки «Лаборатории Касперского».

3.2.2.1. Выбор способа активации приложения

В зависимости от того, есть ли у вас ключ для Антивируса Касперского или требуется получить его с сервера «Лаборатории Касперского», вам предлагается несколько способов активации приложения:

- ④ **Активировать, используя код активации.** Выберите этот вариант активации, если вы приобрели коммерческую версию приложения, и вам был предоставлен код активации. На основании этого кода вы получите файл ключа, обеспечивающий доступ к полной функциональности приложения на весь период действия лицензионного соглашения.
- ④ **Активировать пробную версию.** Выберите данный вариант активации, если вы хотите установить пробную версию приложения перед принятием решения о покупке коммерческой версии. Вам будет предоставлен бесплатный ключ со сроком действия, ограниченным лицензионным соглашением для пробной версии приложения.
- ④ **Использовать полученный ранее ключ.** Активируйте приложение с помощью полученного ранее файла ключа для Антивируса Касперского 7.0.
- ④ **Активировать приложение позже.** При выборе этого варианта этап активации приложения будет пропущен. Антивирус Касперского 7.0 будет установлен на ваш компьютер, вам будут доступны все функции приложения, за исключением обновления (обновить приложение вы сможете только один раз после установки).

3.2.2.2. Ввод кода активации

Для активации приложения требуется ввести код активации. При покупке приложения через интернет код активации отправляется вам по электронной почте. В случае покупки приложения в коробке, код активации указан на конверте с установочным диском.

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 ваши номер клиента и пароль, если вы уже проходили процедуру регистрации клиентов «Лаборатории Касперского» и у вас есть эти данные. Если вы еще не регистрировались, оставьте поля пустыми. В этом случае на следующем этапе мастер активации запросит вашу контактную информацию и выполнит регистрацию. По окончании регистрации вам будут присвоены номер клиента и пароль, которые являются обязательным условием для получения технической поддержки. При регистра-

ции через мастер активации номер клиента можно будет посмотреть в разделе **Поддержка** (см. п. 15.10 на стр. 206) главного окна приложения.

3.2.2.3. Регистрация пользователя

На данном шаге мастера активации требуется указать вашу контактную информацию: адрес электронной почты, страну и город проживания. Данная информация требуется Службе технической поддержки «Лаборатории Касперского» для идентификации вас как зарегистрированного пользователя.

После ввода информации мастер активации отправит ваши данные на сервер активации, после чего вам будет присвоен номер клиента и пароль к Персональному кабинету на веб-сайте Службы технической поддержки. Информацию о номере клиента вы можете получить в разделе **Поддержка** главного окна приложения.

3.2.2.4. Получение файла ключа

Мастер настройки осуществляет соединение с серверами «Лаборатории Касперского» в интернете, отправляет ваши регистрационные данные (код активации, контактную информацию), которые будут проверены на сервере.

В случае успешной проверки кода активации мастер получает файл ключа. Если вы устанавливаете пробную версию приложения, мастер настройки получит файл пробного ключа без кода активации.

Полученный файл будет автоматически установлен для работы приложения, и вы увидите окно завершения активации с подробной информацией об используемом ключе.

Если код активации не пройдет проверку, на экране появится соответствующее уведомление. В данном случае обратитесь за информацией в компанию, где вы приобрели приложение.

3.2.2.5. Выбор файла ключа

Если у вас имеется файл ключа для Антивируса Касперского 7.0, в данном окне мастера вам будет предложено установить его. Для этого воспользуйтесь кнопкой **Обзор** и в стандартном окне выбора файла выберите файл с расширением *.key*.

После успешной установки ключа в нижней части окна будет представлена информации об используемом ключе: имя владельца, номер ключа, его тип (коммерческий, для бета-тестирования, пробный и т.д.), а также дата окончания срока действия ключа.

3.2.2.6. Завершение активации приложения

Мастер настройки информирует вас об успешном завершении активации приложения. Кроме того, приводится информация об установленном ключе: имя владельца, номер ключа, его тип (коммерческий, для бета-тестирования, пробный и т.д.), а также дата окончания срока действия ключа.

3.2.3. Выбор режима защиты

В данном окне мастера настройки вам предлагается выбрать режим защиты, в котором будет работать приложение:

Базовый. Этот режим установлен по умолчанию и предназначен для большинства пользователей, не имеющих достаточного опыта работы с компьютером и антивирусными продуктами. Он подразумевает работу компонентов приложения на рекомендуемом уровне безопасности и информирование пользователя о возникновении только опасных событий (например, обнаружение вредоносного объекта, выполнение опасных действий).

Интерактивный. Этот режим предполагает расширенную защиту данных компьютера по сравнению с базовой защитой. Он позволяет отслеживать попытки изменения системных настроек, подозрительную активность в системе.

Все перечисленные выше действия могут являться результатом деятельности вредоносных программ, так и быть стандартными в рамках работы программ, используемых на вашем компьютере. В каждом отдельном случае вам понадобится принять решение о допустимости или недопустимости тех или иных действий.

При выборе этого режима укажите, в каких случаях он должен использоваться:

- Включить мониторинг системного реестра** – выводить запрос действий пользователя при обнаружении попыток изменения объектов системного реестра.

Если приложение установлено на компьютер под управлением Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista и Microsoft Windows Vista x64, перечисленные далее параметры интерактивного режима отсутствуют.

- Включить контроль целостности приложений** – запрашивать подтверждение действий пользователя при попытке загрузки модулей в контролируемые приложения.

- Включить расширенную проактивную защиту** – включить анализ всей подозрительной активности приложений в системе, в том числе запуск браузера с параметрами командной строки, внедрение в процессы программ и внедрение оконных перехватчиков (по умолчанию данные параметры отключены).

3.2.4. Настройка параметров обновления

Качество защиты вашего компьютера напрямую зависит от своевременного получения обновлений баз и модулей приложения. В данном окне мастера настройки вам предлагается выбрать режим обновления приложения 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 приложение скачивает их и устанавливает на компьютер. Такой режим используется по умолчанию.
- Каждый день в 15:00** (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 приложения.

Обратите внимание, что базы и модули приложения, входящие в дистрибутив, могут устареть на момент установки приложения. Поэтому мы рекомендуем получить самые последние обновления приложения. 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 ваш компьютер.

Если вы хотите перейти к настройке параметров обновления (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**.

3.2.5. Настройка расписания проверки на вирусы

Поиск вредоносных объектов в заданных областях проверки – одна из важных задач, обеспечивающих защиту вашего 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:

Проверка объектов автозапуска

По умолчанию проверка объектов автозапуска производится автоматически при запуске Антивируса Касперского. Параметры расписания можно изменить в окне, открываемом по кнопке **Изменить**.

Проверка критических областей

Для автоматического запуска проверки на вирусы критических областей компьютера (системной памяти, объектов автозапуска, загрузочных секторов, системных каталогов Microsoft Windows) установите флажок в соответствующем блоке. Параметры расписания можно настроить в окне, открываемом по кнопке **Изменить**.

По умолчанию автоматический запуск данной задачи отключен.

Полная проверка компьютера

Для автоматического запуска полной проверки вашего компьютера на вирусы установите флажок в соответствующем блоке. Параметры расписания можно настроить в окне, открываемом по кнопке **Изменить**.

По умолчанию запуск данной задачи по расписанию отключен. Однако мы рекомендуем сразу после установки приложения запустить полную проверку компьютера на вирусы.

3.2.6. Ограничение доступа к приложению

В связи с тем, что персональный компьютер может использоваться несколькими людьми, в том числе с разным уровнем компьютерной грамотности, а также в связи с возможностью отключения защиты со стороны вредоносных программ, вам предлагается ограничить доступ к Антивирусу Касперского с помощью пароля. Пароль позволяет защитить приложение от попыток несанкционированного отключения защиты или изменения ее параметров.

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 инициировании любого действия пользователя с приложением, за исключением работы с уведомлениями об обнаружении опасных объектов.
- Отдельные операции:**
 - Изменение параметров работы приложения** – запрос пароля при попытке пользователя сохранить изменения параметров приложения.
 - Завершение работы с приложением** – запрос пароля при попытке пользователя завершить работу приложения.
 - Остановка / приостановка компонентов защиты и задач проверки** – запрос пароля при попытке пользователя приостановить или выключить полностью работу какого-либо компонента постоянной защиты либо задачи поиска вирусов.

3.2.7. Контроль целостности приложений

На данном этапе работы мастера Антивирус Касперского проанализирует установленные на вашем компьютере приложения (файлы динамических библиотек, цифровые подписи производителей), выполнит подсчет контрольных сумм файлов приложений и создаст список доверенных, с точки зрения антивирусной безопасности, программ. Например, в данный список автоматически будут помещены все приложения, имеющие подпись Microsoft Corporation.

В дальнейшем, полученная в ходе анализа структуры приложений, информация будет использоваться Антивирусом Касперского для предотвращения внедрения вредоносного кода в модули приложений.

Анализ установленных на вашем компьютере приложений может занять некоторое время.

3.2.8. Завершение работы мастера настройки

В последнем окне мастера вам предлагается перезагрузить компьютер для завершения установки приложения. Перезагрузка необходима для корректной регистрации драйверов Антивируса Касперского.

Вы можете отложить перезагрузку компьютера, но в этом случае некоторые компоненты защиты приложения не будут работать.

3.3. Процедура установки приложения из командной строки

Для того чтобы установить Антивирус Касперского 7.0, наберите в командной строке:

```
msiexec /i <имя_пакета>
```

Будет запущен мастер установки (см. п. 3.1 на стр. 31). По завершении установки приложения, необходимо перезагрузить компьютер.

Также вы можете при установке приложения воспользоваться одним из следующих способов.

Чтобы установить приложение в скрытом режиме без перезагрузки компьютера (перезагрузку следует произвести вручную после установки), наберите:

```
msiexec /i <имя_пакета> /qn
```

Чтобы установить приложение в скрытом режиме с последующей перезагрузкой компьютера, наберите:

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

ГЛАВА 4. ИНТЕРФЕЙС ПРИЛОЖЕНИЯ

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

- значок в системной панели (см. п. 4.1 на стр. 44);
- контекстное меню (см. п. 4.2 на стр. 45);
- главное окно (см. п. 4.3 на стр. 47);
- окно настройки параметров приложения (см. п. 4.4 на стр. 50).

Кроме основного интерфейса приложение имеет компоненты расширения (плагины), встраиваемые в приложения:

- Microsoft Office Outlook (см. п. 8.2.2 на стр. 102).
- Microsoft Outlook Express (Windows Mail) (см. п. 8.2.2 на стр. 102).
- The Bat! (см. п. 8.2.3 на стр. 103).
- Microsoft Internet Explorer (см. Глава 9 на стр. 109).
- Microsoft Windows Explorer (см. п. 11.2 на стр. 138).

Плагины расширяют возможности перечисленных программ, позволяя из их интерфейса осуществлять управление и настройку соответствующих компонентов Антивируса Касперского.

4.1. Значок в системной панели

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 приложением.

Если значок активный  (цветной), это означает, что защита вашего компьютера включена. Если значок неактивный  (черно-белый), значит защита выключена полностью или отключены некоторые компоненты защиты (см. п. 2.2.1 на стр. 24).

В зависимости от выполняемой операции значок Антивируса Касперского меняется:



выполняется проверка почтового сообщения;



выполняется проверка скрипта;



выполняется проверка файла, который открываете, сохраняете или запускаете вы или некоторая программа;



выполняется обновление баз и модулей приложения Антивируса Касперского.



произошел сбой в работе какого-либо компонента Антивируса Касперского.

Также значок обеспечивает доступ к основным элементам интерфейса приложения: контекстному меню (см. п. 4.2 на стр. 45) и главному окну (см. п. 4.3 на стр. 47).

Чтобы открыть контекстное меню, щелкните правой клавишей мыши по значку приложения.

Чтобы открыть главное окно Антивируса Касперского на разделе **Защита** (с него по умолчанию начинается работа с приложением), дважды щелкните левой клавишей мыши по значку приложения. Однократное нажатие приведет к открытию главного окна на разделе, который был активен при закрытии.

При появлении новостей от «Лаборатории Касперского» в системной панели появляется значок . Щелкните по нему дважды левой клавишей мыши и в открывшемся окне ознакомьтесь с текстом новости.

4.2. Контекстное меню

Контекстное меню (см. рис. 1) позволяет перейти к выполнению основных задач защиты.

Меню Антивируса Касперского содержит следующие пункты:

Проверка Моего Компьютера – запуск полной проверки вашего компьютера на присутствие вредоносных объектов. В результате будут проверены объекты на всех дисках, в том числе и сменных носителях.

Поиск вирусов – переход к выбору объектов и запуску проверки на вирусы. По умолчанию список содержит ряд объектов, таких как каталог **Мои Документы**, объекты автозапуска, почтовые базы, все

диски вашего компьютера и т.д. Вы можете пополнить список, выбрать объекты для проверки и запустить поиск вирусов.

Обновление – запуск обновления баз и модулей Антивируса Касперского и их установка на вашем компьютере.

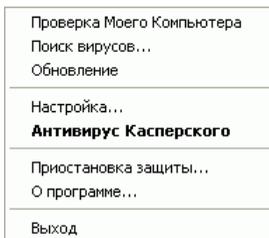


Рисунок 1. Контекстное меню

Активация – переход к активации приложения. Для получения статуса зарегистрированного пользователя, на основании которого вам будут доступны полная функциональность приложения и сервисы Службы технической поддержки, необходимо активировать вашу версию Антивируса Касперского. Данный пункт меню присутствует только в том случае, если приложение не активирована.

Настройка – переход к просмотру и настройке параметров работы Антивируса Касперского.

Антивирус Касперского – открытие главного окна приложения (см. п. 4.3 на стр. 47).

Приостановка защиты / Включение защиты – выключение на время/ включение работы компонентов постоянной защиты (см. п. 2.2.1 на стр. 24). Данный пункт меню не влияет на обновление приложения и на выполнение задач поиска вирусов.

О программе – вызов информационного окна об Антивирусе Касперского.

Выход – завершить работу Антивируса Касперского (при выборе данного пункта меню приложение будет выгружено из оперативной памяти компьютера).

Если в данный момент запущена какая-либо задача поиска вирусов, 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.

4.3. Главное окно приложения

Главное окно Антивируса Касперского (см. рис. 2) условно можно разделить на три части:

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

Существует три возможных состояния защиты (см. п. 5.1 на стр. 52), каждое из которых наглядно выражено определенным цветом, аналогично сигналам дорожного светофора. Зеленый цвет обозначает, что защита вашего компьютера осуществляется на должном уровне, желтый и красный цвета сигнализируют о наличии разного рода проблем в настройке параметров или работе Антивируса Касперского.

Для получения подробной информации об этих проблемах и быстрого их решения воспользуйтесь Мастером безопасности, который открывается по ссылке с уведомлением об угрозах безопасности;

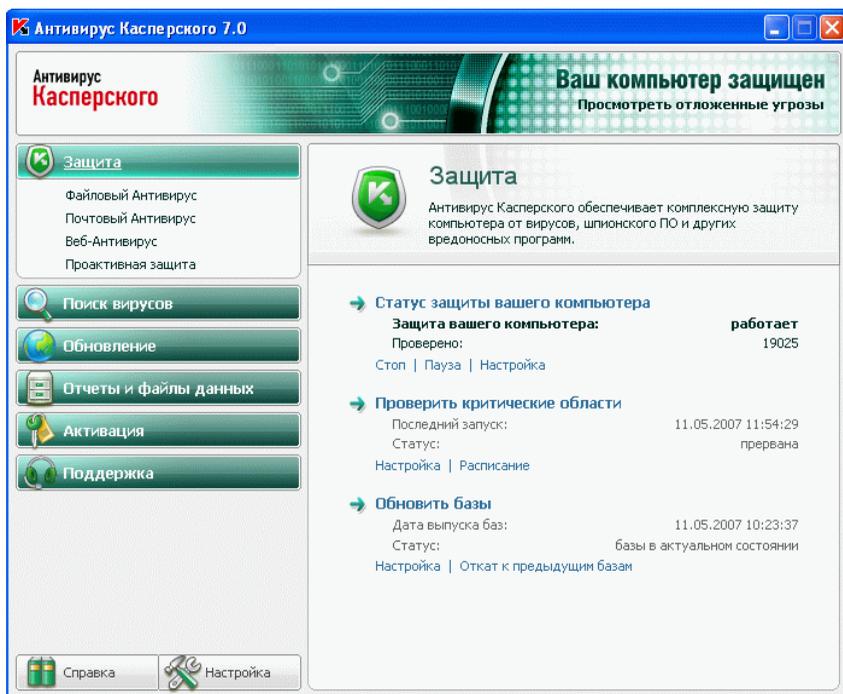
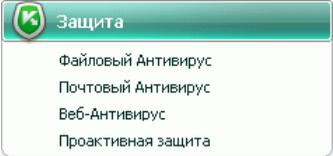
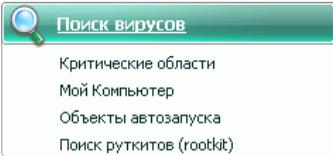


Рисунок 2. Главное окно Антивируса Касперского

- левая часть окна – *навигационная* – позволяет быстро и просто перейти к любому компоненту, к выполнению задач поиска вирусов, обновления, к сервисным функциям приложения;
- правая часть окна – *информационная* – содержит информацию по выбранному в левой части компоненту защиты, позволяет перейти к настройке каждого из них, предоставляет инструменты для выполнения задач поиска вирусов, для работы с файлами на карантине и резервными копиями, для управления лицензионными ключами и т.д.

Выбрав в левой части окна какой-либо раздел или компонент, в правой части вы получите полную информацию, соответствующую сделанному выбору.

Рассмотрим подробнее элементы навигационной панели главного окна.

Раздел навигационной части главного окна	Назначение
	<p>Главная задача раздела Защита – обеспечение доступа к основным компонентам постоянной защиты вашего компьютера.</p> <p>Чтобы просмотреть информацию о работе какого-либо компонента защиты или его модулей, перейти к настройке его параметров или открыть отчет по нему, выберите данный компонент в списке раздела Защита.</p> <p>Кроме того, в данном разделе размещены ссылки, обеспечивающие доступ к наиболее востребованным задачам: проверка объектов на вирусы и обновление баз приложения. Вы можете посмотреть информацию о состоянии данных задач, перейти к их настройке либо сразу запустить их на выполнение.</p>
	<p>Раздел Поиск вирусов обеспечивает доступ к задачам проверки объектов на вирусы. В нем представлены задачи, сформированные экспертами «Лаборатории Касперского», (поиск вирусов в критических областях, среди объектов автозапуска, полная проверка компьютера, поиск руткитов), а также пользова-</p>

Раздел навигационной части главного окна	Назначение
	<p>тельские задачи.</p> <p>При выборе задачи в списке в правой части окна вы можете просмотреть информацию о выполнении данной задачи, перейти к настройке ее параметров, формированию списка объектов для проверки, запустить задачу на выполнение.</p> <p>Для проверки отдельного объекта (файла, папки или диска) выберите раздел Поиск вирусов, в правой части окна добавьте объект в список объектов для проверки и запустите задачу.</p> <p>Кроме того, данный раздел обеспечивает доступ к созданию диска аварийного восстановления (см. п. 15.4 на стр. 185).</p>
	<p>Раздел Обновление содержит информацию об обновлении приложения: дату создания баз и количество сигнатур вирусов, содержащихся в базах.</p> <p>С помощью соответствующих ссылок вы можете запустить обновление, просмотреть детальный отчет, перейти к настройке параметров обновления, выполнить откат обновления до предыдущей версии.</p>
	<p>В разделе Отчеты и файлы данных вы можете просмотреть подробный отчет о работе любого компонента приложения, задачи поиска вирусов или обновления (см. п. 15.3 на стр. 177), а также перейти к работе с объектами, находящимися на карантине (см. п. 15.1 на стр. 171) либо в резервном хранилище (см. п. 15.2 на стр. 175).</p>
	<p>Раздел Активация предназначен для работы с ключами, необходимыми для полнофункциональной работы приложе-</p>

Раздел навигационной части главного окна	Назначение
	<p>ния (см. п. Глава 14 на стр. 168).</p> <p>Если ключ не установлен, рекомендуется как можно скорее приобрести его и активировать приложение (см. п. 3.2.2 на стр. 36).</p> <p>Если ключ установлен, в данном разделе представлена информация о типе используемого ключа и сроке его действия. По истечении срока действия текущего ключа вы можете продлить его через веб-сайт «Лаборатории Касперского».</p>
	<p>В разделе Поддержка представлена информация о сервисах Службы технической поддержки для зарегистрированных пользователей Антивируса Касперского.</p>

Каждый элемент навигационной части сопровождается специальным контекстным меню. Так, для компонентов защиты меню содержит пункты, позволяющие быстро перейти к их настройке, к управлению, к просмотру отчета. Для задач поиска вирусов предусмотрен дополнительный пункт меню, позволяющий на основе выбранной задачи создавать собственную.

Вы можете менять внешний вид приложения, создавая и используя свои графические элементы и цветовую палитру.

В левой нижней части окна расположены две кнопки: **Справка**, обеспечивающая доступ к справочной системе Антивирус Касперского, и **Настройка**, открывающая окно настройки параметров приложения.

4.4. Окно настройки параметров приложения

Окно настройки параметров Антивируса Касперского можно вызвать из главного окна (см. п. 4.3 на стр. 47) или контекстного меню приложения (см. п. 4.2 на стр. 45). Для этого нажмите на кнопку **Настройка** в нижней части главного окна либо выберите одноименный пункт в контекстном меню приложения.

Окно настройки (см. рис. 3) построено аналогично главному окну:

- левая часть окна обеспечивает быстрый и удобный доступ к настройке каждого из компонентов постоянной защиты, задач поиска вирусов, обновления, а также настройке сервисных функций приложения;
- правая часть окна содержит непосредственно перечень параметров выбранного в левой части компонента, задачи и т.д.

При выборе в левой части окна настройки какого-либо раздела, компонента либо задачи в правой части окна будут представлены его основные параметры. Для детальной настройки некоторых параметров вам будет предложено открыть окна настройки второго и третьего уровней. Подробное описание настройки параметров приложения будет приведено в разделах данного Руководства.

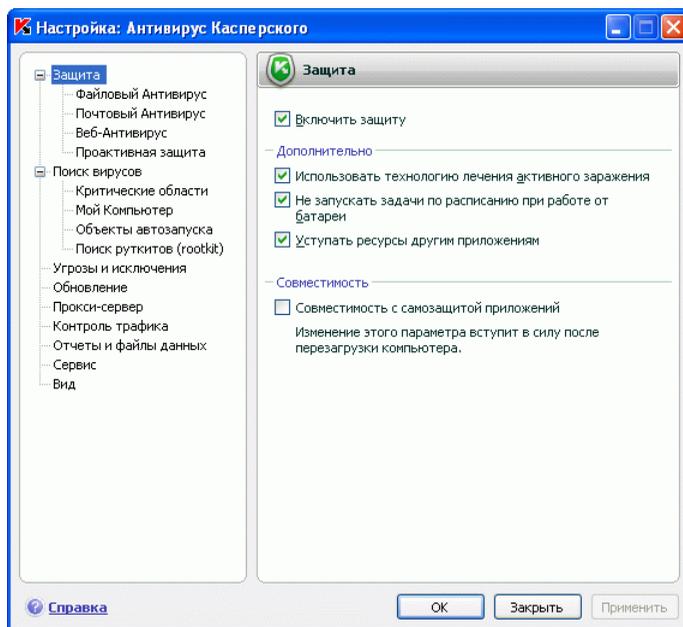


Рисунок 3. Окно настройки Антивируса Касперского

ГЛАВА 5. НАЧАЛО РАБОТЫ

Одной из главных задач специалистов «Лаборатории Касперского» при создании Антивируса Касперского являлась оптимальная настройка всех параметров приложения. Это дает возможность пользователю с любым уровнем компьютерной грамотности, не углубляясь в параметры, обеспечить безопасность компьютера сразу же после установки приложения.

Однако особенности конфигурации вашего компьютера или задач, решаемых на нем, могут иметь некоторую специфику. Поэтому мы рекомендуем вам провести предварительную настройку приложения, чтобы максимально гибко подойти к защите именно вашего компьютера.

Для удобства пользователей мы постарались объединить этапы предварительной настройки в едином интерфейсе мастера первоначальной настройки (см. п. 3.2 на стр. 35), который запускается в конце процедуры установки приложения. Следуя указаниям мастера, вы сможете провести активацию приложения, настроить параметры обновления и запуска задач поиска вирусов, ограничить доступ к приложению с помощью пароля.

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

- Оценить текущий статус защиты, чтобы убедиться, что Антивирус Касперского обеспечивает защиту на должном уровне (см. п. 5.1 на стр. 52).
- Обновить приложение, если это не было сделано с помощью мастера настройки либо автоматически сразу после установки приложения (см. п. 5.6 на стр. 57).
- Проверить компьютер на присутствие вирусов (см. п. 5.3 на стр. 55).

5.1. Каков статус защиты компьютера

Статус защиты вашего компьютера наглядно отражает наличие или отсутствие в данный момент угроз, влияющих на общий уровень безопасности системы. К угрозам в данном случае относится не только обнаружение вредоносных программ, но и использование устаревших баз приложения, отключение некоторых компонентов защиты, использование минимальных параметров работы приложения и др.

Статус защиты представлен в верхней части главного окна приложения и выражен цветом аналогично сигналам светофора. В зависимости от ситуации цветовая гамма верхней части окна будет изменяться, а при наличии

угроз в системе безопасности цвет будет дополняться информационным текстом, выполненным в виде ссылки на Мастер безопасности.

Цветовое выражение статуса защиты может принимать одно из следующих значений:

- Основной цвет главного окна – *зеленый*. Этот статус свидетельствует о том, что защита вашего компьютера обеспечивается на должном уровне.

То есть вы своевременно обновили базы приложения, все компоненты защиты включены, приложение работает с параметрами, рекомендуемыми специалистами «Лаборатории Касперского», в результате выполнения задачи полной проверки компьютера не было обнаружено вредоносных объектов либо обнаруженные вредоносные объекты были обезврежены.

- Основной цвет главного окна – *желтый*. Уровень защиты вашего компьютера снижен по сравнению с предыдущим статусом. Данный статус защиты свидетельствует о наличии некоторых проблем в работе или настройке приложения.

Например, есть незначительные отклонения от рекомендуемого режима работы, базы приложения не обновлялись в течение нескольких дней.

- Основной цвет главного окна – *красный*. Ваш компьютер подвергается серьезной угрозе заражения. Этот статус сигнализирует о наличии проблем, которые могут привести к заражению компьютера и потере данных.

Например, произошел сбой в работе одного или нескольких компонентов защиты, приложение не обновлялось очень давно или были обнаружены вредоносные объекты, которые необходимо срочно обезвредить, приложение не активировано.

При наличии проблем в системе защиты рекомендуется немедленно устранить их. Для этого воспользуйтесь Мастером безопасности, который открывается по информационной ссылке о наличии угроз в системе безопасности. Мастер безопасности поможет вам последовательно просмотреть имеющиеся угрозы и перейти к их непосредственному устранению. Степень серьезности угрозы символизируется цветом индикатора:



– индикатор обращает ваше внимание на наличие не критических угроз, которые, однако, могут снизить общий уровень защиты компьютера. Пожалуйста, внимательно отнеситесь к рекомендациям специалистов «Лаборатории Касперского».



– индикатор отражает наличие серьезных угроз для защиты вашего компьютера. Пожалуйста, строго следуйте рекомендациям, приведен-

ным ниже. Все они направлены на повышение защиты вашего компьютера. Рекомендуемые действия оформлены в виде ссылок.

Для того чтобы просто ознакомиться со списком существующих угроз, воспользуйтесь ссылкой [Далее](#). Для каждой угрозы дается ее подробное описание и предлагаются следующие варианты действий:

- *Устранить угрозу немедленно.* Воспользовавшись соответствующими ссылками, вы можете перейти к непосредственному устранению угрозы. Для получения подробной информации о связанных с появлением данной угрозы событиях вы можете просмотреть файл отчета. Немедленное устранение угрозы является рекомендуемым действием.
- *Отложить устранение угрозы.* Если по какой-либо причине вы не можете устранить угрозу немедленно, возможно отложить данное действие и вернуться к нему позже. Для этого воспользуйтесь ссылкой [Отложить](#).

Обратите внимание, что для серьезных угроз данная возможность не предусмотрена. К таким угрозам относятся, например, наличие небезвреженных вредоносных объектов, сбоя в работе одного или нескольких компонентов, повреждение файлов баз приложения.

Если по завершении работы с Мастером безопасности у вас остались неустраненные угрозы, то в верхней части главного окна приложения появится напоминание о необходимости их устранить. При повторном открытии Мастера безопасности отложенные угрозы не будут присутствовать в списке активных угроз. Тем не менее вы можете вернуться к просмотру и устранению отложенных угроз, нажав на ссылку [Просмотреть отложенные угрозы](#) в заключительном окне Мастера.

5.2. Каков статус отдельного компонента защиты о

Для просмотра текущего статуса любого из компонентов постоянной защиты откройте главное окно приложения и в разделе **Защита** выберите компонент. В правой части окна будет представлена сводная информация о работе выбранного компонента.

Самым важным является статус работы компонента:

- *<имя компонента> : работает* – защита, обеспечиваемая данным компонентом, выполняется на должном уровне.
- *<имя компонента> : пауза* – компонент выключен на некоторый промежуток времени. Защита будет возобновлена автоматически по истечении заданного периода или после перезагрузки приложения. Вы

самостоятельно можете включить компонент. Для этого воспользуйтесь ссылкой [Возобновить работу](#).

- *<имя компонента> : выключено* – работа компонента остановлена пользователем. Вы можете включить защиту. Для этого воспользуйтесь ссылкой [Включить](#).
- *<имя компонента> : не работает* – защита, обеспечиваемая данным компонентом, не доступна по каким-либо причинам.
- *<имя компонента> : сбой в работе* – компонент завершил работу в связи с ошибкой.

Если в работе компонента возникла ошибка, попробуйте запустить его еще раз. Если попытка повторного запуска также завершится с ошибкой, просмотрите отчет о работе компонента, возможно там вы сможете найти причину сбоя. Если же вы не можете самостоятельно разобраться в проблеме, сохраните отчет о работе компонента в файл по кнопке **Действия** → **Сохранить как** и обратитесь в Службу технической поддержки «Лаборатории Касперского».

Вслед за статусом работы компонента может быть приведена информация о настройках, с которыми работает компонент (например, уровень безопасности, действие, которое должно быть применено к опасным объектам). Если в состав компонента входят несколько модулей, приводится информация об их состоянии: включены или выключены. Для перехода к редактированию текущих параметров работы компонента воспользуйтесь ссылкой [Настроить](#).

Кроме того, вынесена некоторая статистика по результатам работы каждого компонента. Для просмотра детального отчета воспользуйтесь ссылкой [Открыть отчет](#).

Если по какой-то причине на данный момент компонент выключен или приостановлен, вы можете ознакомиться с результатами его работы на момент выключения. Для этого воспользуйтесь ссылкой [Открыть отчет о последнем запуске](#).

5.3. Как проверить на вирусы компьютер

После установки приложение обязательно уведомит вас сообщением в нижней левой части окна приложения специальным сообщением о том, что проверка компьютера еще не выполнялась, и порекомендует немедленно проверить его на вирусы.

В поставку Антивируса Касперского включена задача поиска вирусов на компьютере. Она расположена в главном окне приложения в разделе **Поиск вирусов**.

Выбрав задачу **Мой Компьютер**, вы можете просмотреть параметры задачи: какой выбран уровень безопасности, какое действие будет применено к опасным объектам, а также открыть отчет о последнем запуске задачи.

Чтобы проверить компьютер на присутствие вредоносных объектов,

1. В главном окне приложения выберите задачу **Мой компьютер** в разделе **Поиск вирусов**.
2. Нажмите на ссылку Запустить проверку.

В результате запустится проверка вашего компьютера, детали которой отображаются в специальном окне. При нажатии на кнопку **Заккрыть** окно с информацией о ходе проверки будет скрыто; при этом проверка остановлена не будет.

5.4. Как проверить критические области компьютера

На вашем компьютере есть области, критические с точки зрения безопасности. Они являются объектом поражения вредоносными программами, нацеленными на повреждение операционной системы вашего компьютера, процессора, памяти и т.д.

Крайне важно защитить критические области компьютера, чтобы сохранить его работоспособность. Для вашего удобства предусмотрена специальная задача поиска вирусов в таких областях. Она расположена в главном окне приложения в разделе **Поиск вирусов**.

Выбрав задачу **Критические области**, вы можете просмотреть параметры задачи: какой выбран уровень безопасности, какое действие применяется к вредоносным объектам. Тут же можно выбрать, какие именно критические области вы хотите проверить и сразу же запустить поиск вирусов в выбранных областях.

Чтобы проверить критические области компьютера на присутствие вредоносных объектов,

1. В главном окне приложения выберите задачу **Критические области** в разделе **Поиск вирусов**.
2. Нажмите на ссылку Запустить проверку.

В результате запустится проверка выбранных областей, детали которой отображаются в специальном окне. При нажатии на кнопку **Заккрыть** окно с информацией о ходе проверки будет скрыто; при этом проверка остановлена не будет.

5.5. Как проверить на вирусы файл, каталог или диск

Бывают ситуации, когда необходимо проверить на присутствие вирусов не весь компьютер, а отдельный объект, например, один из жестких дисков, на котором находятся программы и игры, почтовые базы, принесенные с работы, пришедший по почте архив и т.п. Выбрать объект для проверки вы можете стандартными средствами операционной системы Microsoft Windows (например, в окне программы **Проводник** или на **Рабочем столе** и т.д.).

Чтобы запустить проверку объекта,

установите курсор мыши на имени выбранного объекта, по правой клавише мыши откройте контекстное меню Microsoft Windows и выберите пункт **Проверить на вирусы** (см. рис. 4).

В результате запустится проверка выбранного объекта, детали которой отображаются в специальном окне. При нажатии на кнопку **Закреть** окно с информацией о ходе проверки будет скрыто; при этом проверка остановлена не будет.

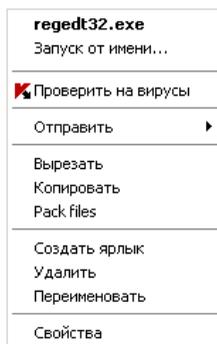


Рисунок 4. Проверка на присутствие вирусов объекта, выбранного средствами Microsoft Windows

5.6. Как обновить приложение

«Лаборатория Касперского» обновляет базы и модули Антивируса Касперского, используя специальные серверы обновлений.

Серверы обновлений «Лаборатории Касперского» – интернет-сайты «Лаборатории Касперского», на которые выкладываются обновления приложения.

Внимание!

Для обновления Антивируса Касперского требуется наличие соединения с интернетом.

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.

Чтобы самостоятельно обновить Антивирус Касперского,

1. В главном окне приложения выберите раздел **Обновление**.
2. Нажмите на ссылку Обновить базы.

В результате запустится обновление Антивируса Касперского. Все детали процесса отображаются в специальном окне.

5.7. Что делать, если защита не работает

В случае возникновения проблем или ошибок в работе какого-либо компонента защиты обязательно обратите внимание на его статус. Если статус компонента *не работает* или *сбой в работе*, попробуйте перезагрузить Антивирус Касперского.

Если после перезапуска приложения проблема не будет решена, рекомендуется исправить возможные ошибки с помощью программы восстановления приложения (см. Глава 17 на стр. 226).

В случае если процедура восстановления приложения не помогла, обратитесь в Службу технической поддержки «Лаборатории Касперского». Возможно вам потребуется сохранить отчет о работе компонента в файл и отправить его сотрудникам Службы технической поддержки для детального ознакомления.

Чтобы сохранить отчет о работе отдельного компонента в файл,

1. Выберите компонент в разделе **Защита** главного окна приложения и воспользуйтесь ссылкой Открыть отчет (в случае, если компонент работает в данный момент) или ссылкой Открыть отчет о последнем запуске (в случае, если компонент выключен).
2. В окне отчета нажмите на кнопку **Действия** → **Сохранить как** и в открывшемся окне укажите имя файла, в котором будут сохранены результаты работы компонента.

ГЛАВА 6. КОМПЛЕКСНОЕ УПРАВЛЕНИЕ ЗАЩИТОЙ

В данном разделе представлена информация по настройке общих параметров приложения, использующихся в работе всех компонентов постоянной защиты и задач, а также по формированию области защиты – перечня угроз, защита от которых будет обеспечиваться приложением, и списка доверенных объектов, исключаемых из защиты:

- управление постоянной защитой компьютера (см. п. 6.1 на стр. 59);
- использование технологии лечения активного заражения (см. п. 6.2 на стр. 63);
- запуск задач при работе на портативном компьютере (см. п. 6.3 на стр. 64);
- совместная работа Антивируса Касперского и других приложений (см. п. 6.4 на стр. 64);
- совместимость Антивируса Касперского с самозащитой других приложений (см. п. 6.5 на стр. 65);
- перечень угроз (см. п. 6.2 на стр. 63), защита от которых будет обеспечиваться приложением;
- список объектов доверенной зоны (см. п. 6.9 на стр. 70), которые будут исключены из защиты.

6.1. Отключение / включение постоянной защиты вашего компьютера

По умолчанию Антивирус Касперского запускается при старте операционной системы, о чем вас информирует надпись *Антивирус Касперского 7.0* в правом верхнем углу экрана, и защищает ваш компьютер в течение всего сеанса работы. Все компоненты постоянной защиты (см. п. 2.2.1 на стр. 24) работают.

Вы можете отключить защиту, обеспечиваемую Антивирусом Касперского, полностью или частично.

Внимание!

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

Обратите внимание, что в данном случае защита рассматривается именно в контексте компонентов защиты. Отключение или приостановка работы компонентов защиты не оказывает влияния на выполнение задач поиска вирусов и обновления приложения.

6.1.1. Приостановка защиты

Приостановка постоянной защиты означает отключение на некоторый промежуток времени всех ее компонентов, контролирующих файлы на вашем компьютере, входящую и исходящую почту, исполняемые скрипты, поведение приложений.

Для того чтобы приостановить постоянную защиту компьютера,

1. В контекстном меню (см. п. 4.2 на стр. 45) приложения выберите пункт **Приостановка защиты**.
2. В открывшемся окне отключения защиты (см. рис. 5) выберите период времени, спустя который защита будет включена:
 - Через <временной интервал> – защита будет включена через указанное время. Для выбора значения временного интервала воспользуйтесь раскрывающимся списком.
 - После перезапуска приложения – защита будет включена, если вы загрузите приложение из меню **Пуск** или после перезагрузки системы (при условии, что включен режим запуска приложения при включении компьютера (см. п. 15.11 на стр. 208).
 - Только по требованию пользователя – защита будет включена только тогда, когда вы сами ее запустите. Для включения защиты выберите пункт **Включение защиты** в контекстном меню приложения.

В результате временного отключения работа всех компонентов постоянной защиты приостанавливается. Об этом свидетельствуют:

- Неактивные (серого цвета) названия выключенных компонентов в разделе **Защита** главного окна.
- Неактивный (серый) значок приложения в системной панели.

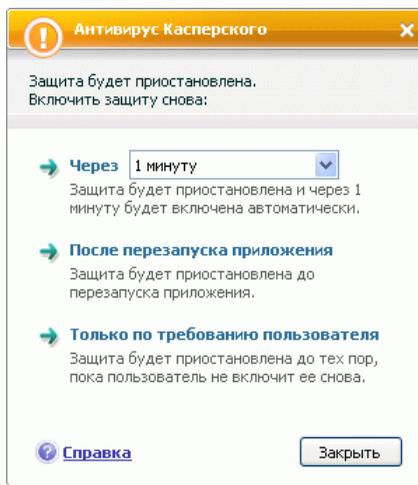


Рисунок 5. Окно приостановки защиты вашего компьютера

6.1.2. Полное отключение защиты компьютера

Полное отключение защиты означает остановку работы компонентов постоянной защиты. Поиск вирусов и обновление продолжают работать в данном режиме.

Если защита отключена полностью, она может быть включена только по требованию пользователя. Автоматического включения компонентов защиты после перезагрузки системы или приложения в этом случае не происходит. Помните, что если Антивирус Касперского каким-либо образом конфликтует с другими программами, установленными на вашем компьютере, вы можете приостановить работу отдельного компонента защиты или сформировать список исключений (см. п. 6.9 на стр. 70).

Чтобы полностью отключить постоянную защиту компьютера,

1. Откройте окно настройки приложения и выберите раздел **Защита**.
2. Снимите флажок **Включить защиту**.

В результате отключения защиты работа всех ее компонентов останавливается. Об этом свидетельствуют:

- Неактивные (серого цвета) названия выключенных компонентов в разделе **Защита** главного окна.
- Неактивный (серый) значок приложения в системной панели.

6.1.3. Приостановка / выключение отдельных компонентов защиты

Отключить работу какого-либо компонента защиты можно несколькими способами. Однако прежде чем делать это, рекомендуем вам определить причину, по которой вы хотите отключить их. Вероятно, это можно решить другим способом, например, изменив уровень безопасности. Так, например, если вы работаете с некоторой базой данных, которая на ваш взгляд не может содержать вирусов, просто укажите каталог с ее файлами в качестве исключения (см. п. 6.9 на стр. 70).

Чтобы приостановить отдельный компонент защиты,

откройте главное окно приложения, выберите компонент в разделе **Защита** и воспользуйтесь ссылкой [Пауза](#).

Статус компонента изменится на *пауза*. Защита, обеспечиваемая компонентом, будет приостановлена до того момента, пока вы не перезагрузите приложение или не включите компонент, нажав на ссылку [Возобновить работу](#).

Когда вы приостанавливаете компонент защиты, статистика в текущем сеансе работы Антивируса Касперского сохраняется и будет продолжаться формироваться после возобновления работы компонента.

Чтобы выключить отдельный компонент защиты,

откройте главное окно приложения, выберите компонент в разделе **Защита** и воспользуйтесь ссылкой [Стоп](#).

В этом случае статус компонента поменяется на *выключен* и в списке компонентов раздела **Защита** его название станет неактивным (серого цвета). Защита, обеспечиваемая компонентом, будет отключена пока вы не нажмете на ссылку [Включить](#).

Отключить любой из компонентов постоянной защиты можно также из окна настройки приложения. Для этого откройте окно настройки, выберите компонент в разделе **Защита** и снимите флажок **Включить <имя компонента>**.

При выключении компонента защиты вся статистика предыдущей работы обнуляется и при запуске компонента будет формироваться заново.

Работа отдельных компонентов защиты также отключается при полном выключении постоянной защиты вашего компьютера (см. п. 6.1.2 на стр. 61).

6.1.4. Возобновление защиты вашего компьютера

Если в какой-либо момент времени вы приостановили или полностью отключили постоянную защиту вашего компьютера, то включить ее вы можете одним из следующих способов:

- Из контекстного меню.

Для этого выберите пункт **Включение защиты**.

- Из главного окна приложения.

Выберите раздел **Защита** в левой части главного окна и воспользуйтесь ссылкой Запуск.

Статус защиты сразу же изменится на *работает*. Значок приложения в системной панели станет активным (цветным).

6.2. Технология лечения активного заражения

Современные вредоносные программы могут внедряться на самые низкие уровни операционной системы, что делает процесс их удаления практически невозможным. Антивирус Касперского 7.0 при обнаружении угрозы, которая в данный момент активна в системе, предлагает провести специальную расширенную процедуру лечения, в результате которой угроза будет обезврежена и удалена с компьютера.

По окончании процедуры будет произведена обязательная перезагрузка компьютера. После перезагрузки компьютера рекомендуется запустить полную проверку на вирусы. Для применения процедуры расширенного лечения откройте окно настройки приложения, выберите раздел **Защита** и установите флажок **Использовать технологию лечения активного заражения** в блоке **Дополнительно** (см. рис. 6).

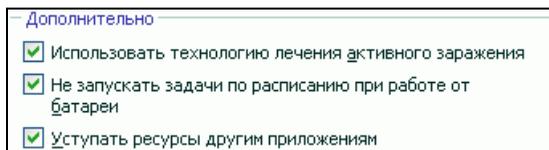


Рисунок 6. Настройка общих параметров

6.3. Работа приложения на портативном компьютере

В целях экономии питания аккумулятора портативного компьютера вы можете отложить выполнение задач поиска вирусов.

Поскольку поиск вирусов на компьютере и обновление приложения подчас требуют достаточного количества ресурсов и занимают некоторое время, рекомендуем вам отключать запуск таких задач по расписанию. Это позволит вам сэкономить заряд аккумулятора. По мере необходимости вы сможете самостоятельно обновить приложение (см. п. 5.6 на стр. 57) или запустить проверку на вирусы (см. п. 5.3 на стр. 55). Чтобы воспользоваться сервисом экономии заряда аккумулятора, откройте окно **настройки приложения**, выберите раздел **Защита** и установите флажок **Не запускать задачи по расписанию при работе от батареи** в блоке **Дополнительно** (см. рис. 6).

6.4. Производительность компьютера при выполнении задач

В целях ограничения нагрузки на центральный процессор и дисковые подсистемы, вы можете отложить выполнение задач поиска вирусов.

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

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Для того чтобы поиск вирусов не зависел от работы таких программ, откройте окно **настройки приложения**, выберите раздел **Защита** и установите флажок **Уступать ресурсы другим приложениям** в блоке **Дополнительно** (см. рис. 6).

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

6.5. Решение проблем совместимости Антивируса Касперского с другими приложениями

В некоторых случаях при использовании Антивируса Касперского возможно возникновение конфликтов в работе с приложениями, установленными на компьютере. Это связано с тем, что данные программы имеют встроенный механизм самозащиты, который срабатывает при попытке внедрения в них Антивируса Касперского. К таким приложениям относятся, например, плагин Authentica к программе Adobe Reader, осуществляющий проверку доступа к документам в pdf-формате, программа для управления мобильными телефонами Oхugen Phone Manager II, а также некоторые виды игр, имеющие защиту от взлома.

Для решения данной проблемы откройте окно настройки приложения, выберите раздел **Защита** и установите флажок **Совместимость с самозащитой приложений** в блоке **Совместимость** (см. рис. 7). Для вступления изменений данного параметра в силу требуется перезагрузка операционной системы.

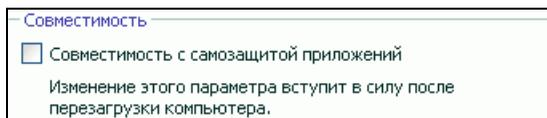


Рисунок 7. Настройка параметров совместимости

6.6. Запуск задач поиска вирусов и обновления с правами другого пользователя

В Антивирусе Касперского 7.0 реализован сервис запуска пользователем задач 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.

Так, например, при выполнении задачи проверки могут потребоваться права на доступ к проверяемому объекту. Используя данный сервис, вы можете настроить запуск задачи от имени пользователя, обладающего такими привилегиями.

Что касается обновления приложения, то оно 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 приложения от имени пользователя, обладающего такими привилегиями.

Чтобы настроить запуск задачи поиска вирусов от имени другой учетной записи,

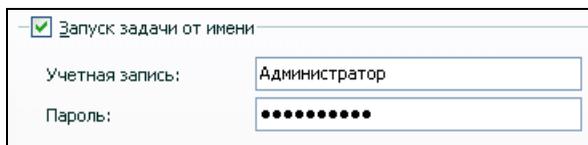
1. Откройте окно настройки приложения и выберите имя задачи в разделе **Поиск вирусов**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** и в открывшемся окне перейдите на закладку **Дополнительно**.

Чтобы настроить запуск задачи обновления от имени другой учетной записи,

1. Откройте окно настройки приложения и выберите раздел **Обновление**.
2. Нажмите на кнопку **Настройка** в блоке **Параметры обновления** и в открывшемся окне перейдите на закладку **Дополнительно** (см. рис. 8).

Для включения данного сервиса установите флажок **Запуск задачи от имени**. Ниже введите данные учетной записи, под которой будет запускаться задача: имя пользователя и пароль.

Обратите внимание, что без использования запуска с правами обновление по расписанию будет выполняться с правами текущей учетной записи. В 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.



The screenshot shows a dialog box titled "Запуск задачи от имени" (Run task as user). At the top left, there is a checked checkbox. Below the title, there are two input fields: "Учетная запись:" (User name) with the text "Администратор" (Administrator) entered, and "Пароль:" (Password) with a series of black dots representing a masked password.

Рисунок 8. Настройка запуска задач от имени другой учетной записи

6.7. Настройка расписания запуска задач и отправки уведомлений

Настройка расписания стандартна для задач поиска вирусов, обновления приложения, а также отправки уведомлений о работе Антивируса Касперского.

Запуск задач поиска вирусов, созданных при установке приложения, по умолчанию отключен. Исключение составляет задача проверки объектов автозапуска, которая выполняется каждый раз при запуске Антивируса Касперского. Что касается обновления, то по умолчанию оно выполняется автоматически по мере выхода обновлений на серверах «Лаборатории Касперского».

Если вас не устраивает такой режим работы задач, отредактируйте параметры их расписания.

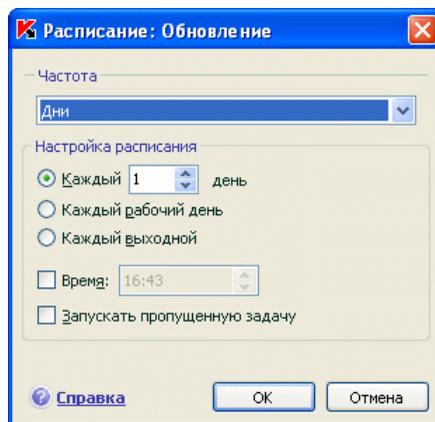


Рисунок 9. Формирование расписания запуска задач

Главное, что вам нужно определить, – это интервал, с которым должно выполняться событие (запуск задачи или отправка уведомления). Для этого выберите в блоке **Частота** (см. рис. 9) требуемый вариант. Далее необходимо указать параметры расписания для выбранного варианта в блоке **Настройка расписания**. На выбор предлагаются следующие варианты:

- В определенное время.** Производить запуск задачи или отставку уведомления в указанные день и время.

- ① **При запуске приложения.** Осуществлять запуск задачи или отправку уведомления при каждом запуске Антивируса Касперского. Дополнительно вы можете указать временной интервал после запуска приложения, по прошествии которого будет выполнен запуск.
- ① **После каждого обновления.** Задача запускается после каждого обновления баз приложения (данный пункт относится только к задачам поиска вирусов).
- ① **Минуты.** Временной интервал между запусками задачи или отправкой уведомлений составляет несколько минут. В параметрах расписания укажите значение интервала в минутах. Оно не должно превышать 59 минут.
- ① **Часы.** Интервал между запусками задачи или отправкой уведомлений исчисляется в часах. Если вы выбрали такую частоту, в параметрах расписания укажите интервал: **Каждый N-й час** и уточните интервал *N*. Например, для ежечасного запуска установите **Каждый 1 час**.
- ① **Дни.** Запуск задачи или отправка уведомлений осуществляется с интервалом в несколько дней. В параметрах расписания определите значение интервала:
 - Выберите вариант **Каждый N-й день** и уточните интервал *N*, если вы хотите соблюдать некоторый интервал в днях.
 - Выберите вариант **Каждый рабочий день**, если вы хотите осуществлять запуск ежедневно с понедельника по пятницу.
 - Выберите **Каждый выходной**, для того чтобы осуществлять запуск только по субботам и воскресеньям.Дополнительно к частоте в поле **Время** укажите, в какое время суток будет производиться запуск задачи проверки.
- ① **Недели.** Запуск задачи или отправка уведомлений осуществляется в определенные дни недели. Если вы выбрали данную частоту, в параметрах расписания установите флажки для тех дней недели, когда требуется выполнять запуск. Дополнительно укажите время в поле **Время**.
- ① **Месяцы.** Запуск задачи или отправка уведомлений выполняется один раз в месяц в указанное время.

Если по каким-либо причинам запуск невозможен (например, не установлена почтовая программа либо в это время компьютер был выключен), вы можете настроить автоматический запуск, как только это станет возможным. Для этого установите флажок **Запускать пропущенную задачу** в окне расписания.

6.8. Типы контролируемых вредоносных программ

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

Чтобы выбрать, от каких видов вредоносных программ будет защищать Антивирус Касперского, откройте окно настройки приложения и выберите раздел **Угрозы и исключения** (см. рис. 10).

Типы угроз (см. п. 1.3 на стр. 12) приведены в блоке **Категории вредоносного ПО**:

- Вирусы, черви, троянские и хакерские программы.** Эта группа объединяет наиболее распространенные и опасные категории вредоносных программ. Защита от них обеспечивает минимально-допустимый уровень безопасности. В соответствии с рекомендациями специалистов «Лаборатории Касперского» Антивирус Касперского всегда контролирует вредоносные программы данной категории.
- Шпионское, рекламное ПО, программы скрытого дозвона.** Данная группа объединяет в себе потенциально опасное программное обеспечение, которое может причинить неудобство пользователю или даже нанести значительный ущерб.
- Потенциально опасное ПО (riskware).** Эта группа включает программы, которые не являются вредоносными или опасными, однако при некотором стечении обстоятельств могут быть использованы для нанесения вреда вашему компьютеру.

Приведенные группы регулируют полноту использования баз приложения при проверке объектов в режиме реального времени и при поиске вирусов на вашем компьютере.

Если выбраны все группы, Антивирус Касперского обеспечивает максимально полную антивирусную защиту вашего компьютера. Если вторая и третья группы отключены, приложение защищает вас только от наиболее распространенных вредоносных объектов. При этом не контролируются потенциально опасные и другие программы, которые могут быть установлены на вашем компьютере и своими действиями наносить моральный или материальный ущерб.

Специалисты «Лаборатории Касперского» не рекомендуют отключать контроль второй группы. При возникновении ситуации, когда Антивирус Кас-

перского относит программу, которая, по вашему мнению, не является опасной, к категории потенциально опасных программ, рекомендуется настроить для нее исключение (см. п. 6.9 на стр. 70).

Для того чтобы выбрать типы контролируемых вредоносных программ, откройте окно настройки приложения и выберите раздел **Угрозы и исключения**. Настройка производится в блоке **Категории вредоносного ПО** (см. рис. 10).

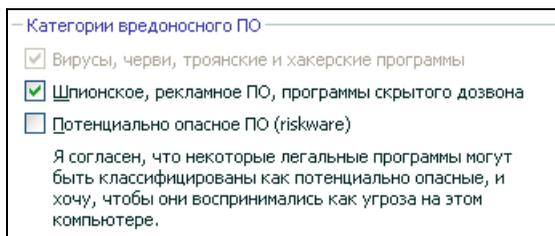


Рисунок 10. Выбор типа контролируемых угроз

6.9. Формирование доверенной зоны

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

Доверенную зону формирует пользователь, исходя из особенностей объектов, с которыми он работает, а также программ, установленных на 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 типу угрозы согласно классификации Вирусной энциклопедии (статусу, который присвоен объекту приложением при проверке).

Внимание!

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,

1. Откройте окно настройки приложения и выберите раздел **Угрозы и исключения** (см. рис. 10).
2. Нажмите на кнопку **Доверенная зона** в блоке **Исключения**.
3. В открывшемся окне (см. рис. 11) настройте правила исключений для объектов, а также сформируйте список доверенных приложений.

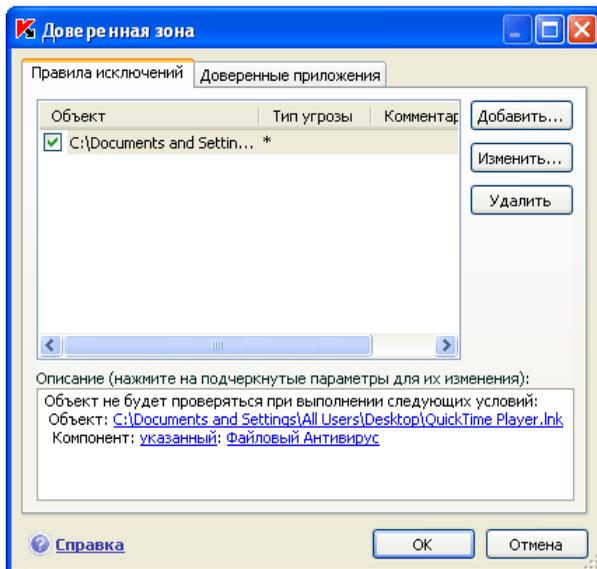


Рисунок 11. Формирование доверенной зоны

6.9.1. Правила исключений

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 типу угрозы согласно 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 остановки 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). В результате проверки такие программы могут быть заблокированы. А поскольку некоторые из них широко используются 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 приложения рассматривается Антивирусом Касперского как потенциально опасная и может быть заблокирована. Чтобы исключить блокировку приложения, нужно сформировать исключяющее правило, где в качестве типа угрозы указать – not-a-virus:RemoteAdmin.Win32.RAdmin.22.

При добавлении исключения формируется правило, которое потом может использоваться некоторыми компонентами приложения (Файловый Антивирус, Почтовый Антивирус, Проактивная защита), а также при выполнении задач поиска вирусов. Правило исключения можно создать в специальном окне, которое можно открыть из окна настройки приложения либо из уведомления об обнаружении объекта, а также из окна отчета.

*Добавление объекта исключения на закладке **Правила исключений**:*

1. Нажмите на кнопку **Добавить** в окне **Правила исключений** (см. рис. 11).
2. В открывшемся окне (см. рис. 12) выберите тип исключения в разделе **Параметры**:

Объект – исключение из проверки определенного объекта, каталога или файлов, соответствующих некоторой маске.

Тип угрозы – исключение из проверки объекта, исходя из его статуса в соответствии с классификацией Вирусной энциклопедии.

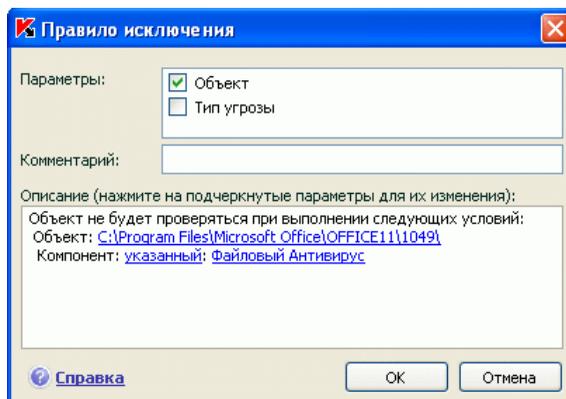


Рисунок 12. Создание правила исключения

Если одновременно установить оба флажка, будет создано правило для указанного объекта с определенным типом угрозы по классификации Вирусной энциклопедии. В этом случае действуют следующие правила:

- Если в качестве **Объекта** указан некоторый файл, а в качестве **Типа угрозы** – определенный статус, то указанный файл будет исключением только в том случае, если ему в процессе проверки будет присвоен статус заданной угрозы.
 - Если в качестве **Объекта** указана некоторая область или папка, а в качестве **Типа угрозы** – статус (или маска), то из проверки исключаются объекты заданного статуса, обнаруживаемые только в указанной области / папке.
3. Задайте значения выбранным типам исключений. Для этого в разделе **Описание** щелкните левой клавишей мыши по ссылке укажите, расположенной рядом с типом исключения:
- Для типа **Объект** в открывшемся окне введите его имя (это может быть файл, некоторая папка или маска файла (см. п. А.2 на стр. 234). Чтобы указанный объект (файл, маска файла, папка) рекурсивно исключался при проверке, установите флажок **Включая вложенные папки**. Например, если в качестве исключения вы задали файл **C:\Program Files\winword.exe** и установили флажок проверки вложенных папок, из проверки будет исключен файл **winword.exe**, расположенный в любой папке каталога **C:\Program Files**.

- Для **Типа угрозы** укажите полное имя исключаемой из проверки угрозы, как оно представлено в Вирусной энциклопедии, либо имя по маске (см. п. А.3 на стр. 235).

Для некоторых объектов, исключаемых по типу угрозы, в поле **Дополнительные параметры** можно задать дополнительные условия применения правила. В большинстве случаев это поле заполняется автоматически при добавлении правила исключения из уведомлений Проактивной защиты.

Указание дополнительных параметров может потребоваться, например, для следующих вердиктов:

- *Invader* (внедрение в процессы программ). Для данного вердикта в качестве дополнительного условия исключения вы можете указать имя, маску либо полный путь к внедряемому объекту (например, файлу dll).

- *Launching Internet Browser* (запуск браузера с параметрами). Для данного вердикта в качестве дополнительного условия исключения вы можете указать параметры запуска браузера.

Например, в анализе активности приложений Проактивной защиты вы запретили запуск браузера с параметрами. Но в качестве правила исключения вы хотите разрешить запуск браузера для домена *www.kaspersky.com* по ссылке из Microsoft Office Outlook. Для этого в качестве **Объекта** исключения укажите программу Microsoft Office Outlook, в качестве **Типа угрозы** укажите *Launching Internet Browser*, а в поле **Дополнительные параметры** введите маску разрешенного домена.

4. Определите, в работе каких компонентов Антивируса Касперского должно быть использовано создаваемое правило. Если выбрано значение любой, данное правило будет применяться для всех компонентов. Если вы хотите ограничить использование правила одним/несколькими компонентами, щелкните по ссылке любой, которая изменится на указанный. В открывшемся окне установите флажки напротив тех компонентов, для которых будет применяться данное исключяющее правило.

Создание правила исключения из уведомления приложения об обнаружении опасного объекта:

1. В окне уведомления (см. рис. 13) воспользуйтесь ссылкой Добавить в доверенную зону.

2. В открывшемся окне убедитесь, что все параметры исключающего правила устраивают вас. Поля с именем объекта и типом угрозы, который присвоен ему, заполняются автоматически на основании информации из уведомления. Для создания правила нажмите на кнопку **ОК**.

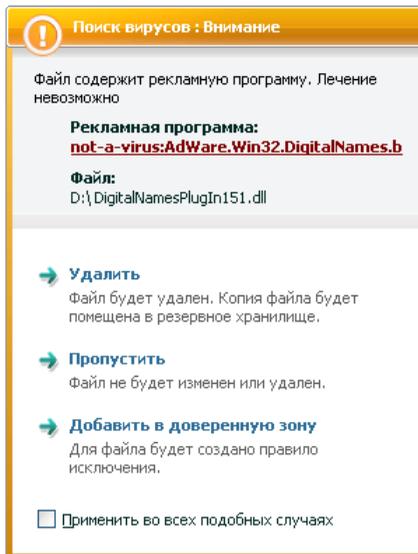


Рисунок 13. Уведомление об обнаружении опасного объекта

Создание правила исключения из окна отчета:

1. Выберите в отчете объект, который вы хотите добавить к исключениям.
2. Откройте контекстное меню и выберите пункт **Добавить в доверенную зону** (см. рис. 14).
3. В результате открывается окно настройки исключения. Убедитесь, что все параметры исключающего правила устраивают вас. Поля с именем объекта и типом угрозы, который присвоен ему, заполняются автоматически на основании информации из отчета. Для создания правила нажмите на кнопку **ОК**.

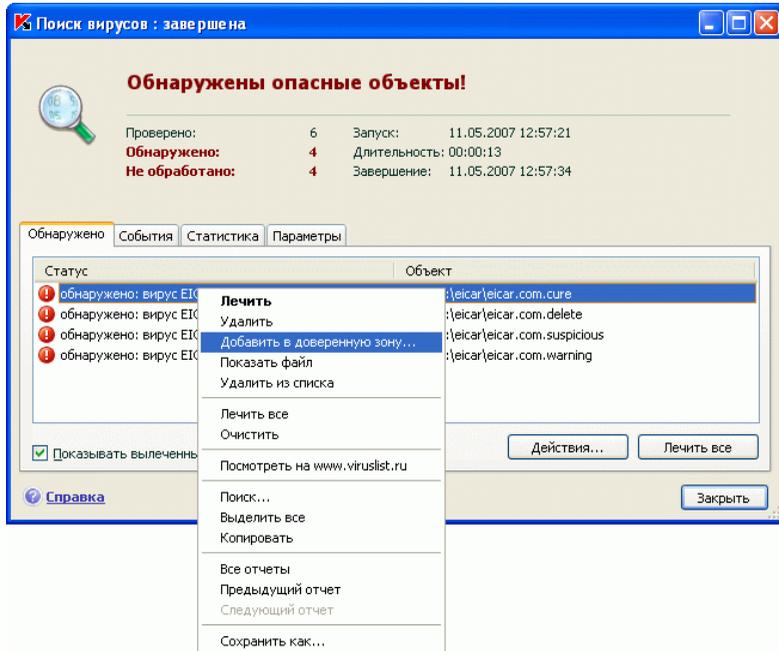


Рисунок 14. Создание правила исключения из отчета

6.9.2. Доверенные приложения

Антивирус Касперского позволяет формировать список доверенных приложений, активность которых, в том числе и подозрительная, а также файловая, сетевая активность и обращение 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 приложений. Однако исполняемый файл и процесс доверенного приложения по-прежнему будут проверяться на вирусы. Для полного исключения приложения из проверки следует пользоваться правилами исключений (см. п. 6.9.1 на стр. 71).

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 приложений из проверки позволяет решать возможные проблемы совместимости Антивируса Касперского с другими приложениями (например, сетевой трафик с другого компьютера, уже проверенный антивирусным приложением), а также увеличить производительность компьютера, что особенно важно при использовании серверных приложений.

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

Формирование списка доверенных приложений осуществляется на специальной закладке **Доверенные приложения** (см. рис. 15). По умолчанию при установке Антивируса Касперского список доверенных приложений содержит приложения, активность которых не анализируется на основании рекомендаций специалистов «Лаборатории Касперского». Если вы считаете, что указанные в списке приложения не являются доверенными, снимите соответствующие флажки. Вы можете отредактировать список с помощью кнопок **Добавить**, **Изменить**, **Удалить**, расположенных справа.

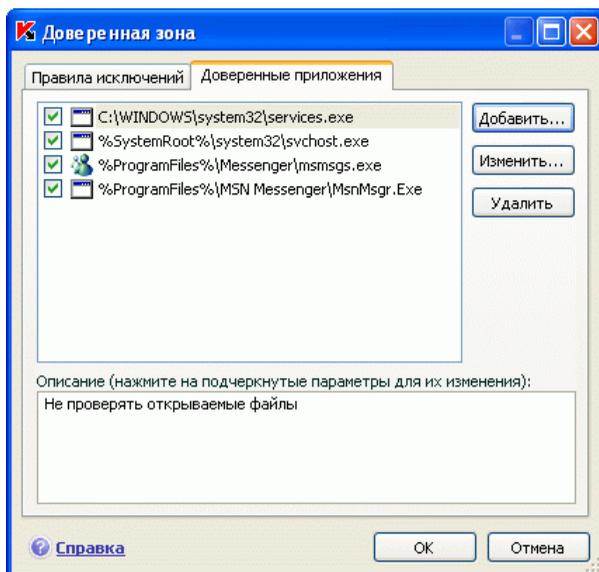


Рисунок 15. Список доверенных приложений

Для того чтобы добавить программу в список доверенных:

1. Нажмите на кнопку **Добавить**, расположенную в правой части закладки **Доверенные приложения**.
2. В открывшемся окне **Доверенное приложение** (см. рис. 16) выберите приложение с помощью кнопки **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 **Приложения** перейти к списку приложений, работающих в данный момент, и выбрать нужное.

При выборе программы Антивирус Касперского запоминает внутренние атрибуты исполняемого файла, по которым идентифицирует программу как доверенную в ходе проверки.

Путь к файлу подставляется автоматически при выборе имени.

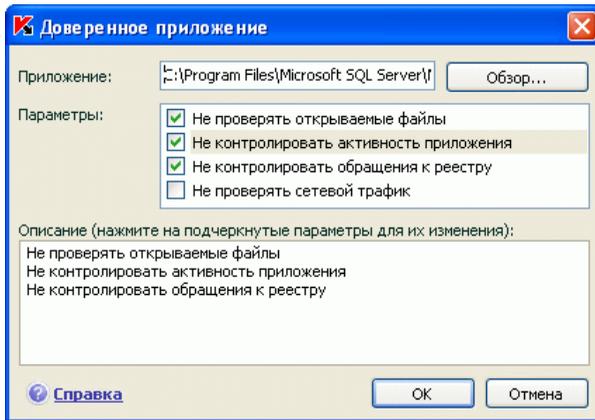


Рисунок 16. Добавление приложения в список доверенных

3. Далее укажите действия, выполняемые данным процессом, которые не будут контролироваться Антивирусом Касперского:
 - Не проверять открываемые файлы** – исключать из проверки все файлы, которые открываются процессом доверенного приложения.
 - Не контролировать активность приложения** – исключать из проверки в рамках работы компонента Проактивная защита любую активность (в том числе и подозрительную), которую выполняет доверенное приложение.
 - Не контролировать обращения к реестру** – исключать из проверки попытки обращения к системному реестру, инициируемые доверенным приложением.

- ✔ **Не проверять сетевой трафик** – исключать из проверки сетевой трафик, инициируемый доверенным приложением. Вы можете исключить из проверки весь сетевой приложения либо только зашифрованный трафик (с использованием протокола SSL). Для этого щелкните по ссылке весь, она изменит свое значение на зашифрованный. Кроме того, вы можете ограничить исключение заданным удаленным хостом/ портом. Для ввода ограничения нажмите на ссылку любой, которая изменится на указанный, и укажите значение удаленного порта / хоста.

ГЛАВА 7. АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВОЙ СИСТЕМЫ КОМПЬЮТЕРА

В состав Антивируса Касперского включен специальный компонент, обеспечивающий защиту файловой системы вашего компьютера от заражения, – *Файловый Антивирус*. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

Индикатором работы компонента является значок Антивируса Касперского в системной панели, который принимает вид  каждый раз при проверке файла.

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

1. Обращение пользователя или некоторой программы к каждому файлу перехватывается компонентом.
2. Файловый Антивирус проверяет наличие информации о перехваченном файле в базах iChecker™ и iSwift™. На основании полученной информации принимается решение о необходимости проверки файла.

Процесс проверки включает следующие действия:

1. Файл анализируется на присутствие вирусов. Распознавание вредоносных объектов происходит на основании *баз приложения*. Базы содержат описание всех известных на настоящий момент вредоносных программ, угроз и способов их обезвреживания.
2. В результате анализа возможны следующие варианты поведения приложения:
 - a. Если в файле обнаружен вредоносный код, Файловый Антивирус блокирует файл, помещает его копию в *резервное хранилище* и пытается вылечить файл. В результате успешного лечения файл становится доступным для работы, если же лечение произвести не удалось, файл удаляется.
 - b. Если в файле обнаружен код, похожий на вредоносный, но стопроцентной гарантии этого нет, файл подвергается ле-

чению и помещается в специальное хранилище – *карантин*.

- c. Если в файле не обнаружено вредоносного кода, он сразу же становится доступным для работы.

7.1. Выбор уровня безопасности файлов

Файловый Антивирус обеспечивает защиту файлов, с которыми вы работаете, на одном из следующих уровней (см. рис. 17):

- **Максимальная защита** – уровень, на котором осуществляется максимально полный контроль за открываемыми, сохраняемыми и запускаемыми файлами.
- **Рекомендуемый**. Параметры данного уровня рекомендованы экспертами «Лаборатории Касперского» и предусматривают проверку следующих категорий объектов:
 - программ и объектов по содержимому;
 - только новых и измененных с момента последней проверки объектов;
 - вложенных OLE-объектов.
- **Максимальная скорость** – уровень с параметрами, которые позволяют вам комфортно работать с приложениями, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых файлов на данном уровне сокращен.

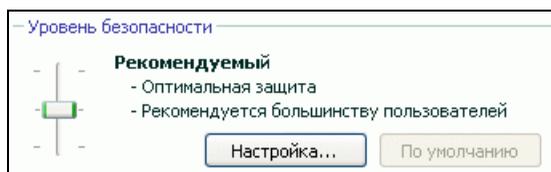


Рисунок 17. Уровни безопасности Файлового Антивируса

По умолчанию защита файлов осуществляется на **Рекомендуемом** уровне.

Вы можете повысить или понизить уровень защиты файлов, с которыми вы работаете, выбрав соответствующий уровень или изменив параметры текущего уровня.

Для того чтобы изменить уровень безопасности,

переместите ползунок по шкале. Регулируя уровень безопасности, вы определяете соотношение между скоростью выполнения проверки и количеством проверяемых файлов: чем меньше файлов подвергается анализу на присутствие вирусов, тем выше скорость проверки.

Если ни один из перечисленных уровней безопасности файлов не соответствует вашим требованиям, вы можете выполнить дополнительную настройку параметров защиты. Для этого рекомендуется выбрать наиболее близкий к вашим пожеланиям уровень в качестве базового и отредактировать его параметры. В этом случае название уровня безопасности будет изменено на **Другой**. Рассмотрим пример, когда может пригодиться изменение параметров предустановленных уровней безопасности.

Пример:

По роду деятельности вы работаете с большим количеством файлов разных типов, в том числе и достаточно большого размера. Вы не хотели бы рисковать, исключая из проверки какие-либо файлы по расширению и размеру, даже если это оказывает некоторое влияние на производительность вашего компьютера.

Совет по выбору уровня:

Основываясь на исходных данных, можно прийти к выводу, что опасность заражения вредоносной программой достаточно высока. Размер и тип используемых в работе файлов достаточно разнообразен и исключать их из проверки – значит подвергнуть риску информацию на компьютере. Основным требованием к проверке является анализ используемых в работе файлов именно по их содержанию, а не по расширению.

В качестве базового предустановленного уровня безопасности рекомендуется использовать **Рекомендуемый** уровень со следующими изменениями: снять ограничение на размер проверяемых файлов и провести оптимизацию работы Файлового Антивируса за счет проверки только новых и измененных файлов. В таком случае нагрузка на компьютер при проверке файлов будет снижена, что позволит комфортно работать с другими приложениями.

Чтобы изменить параметры текущего уровня безопасности,

1. Откройте окно настройки приложения и выберите компонент **Файловый Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 17).
3. В открывшемся окне отредактируйте параметры защиты файлов и нажмите на кнопку **ОК**.

7.2. Настройка защиты файлов

То, каким образом осуществляется защита файлов на вашем компьютере, определяется набором параметров. Их можно разбить на следующие группы:

- параметры, определяющие типы файлов, подвергаемые анализу на вирусы (см. п. 7.2.1 на стр. 83);
- параметры, формирующие защищаемую область (см. п. 7.2.2 на стр. 86);
- параметры, задающие действия над опасным объектом (см. п. 7.2.6 на стр. 93);
- параметры, определяющие использование методов эвристического анализа (см. п. 7.2.4 на стр. 90);
- дополнительные параметры работы Файлового Антивируса (см. п. 7.2.3 на стр. 88).

В данном разделе Руководства будут детально рассмотрены все перечисленные выше группы.

7.2.1. Определение типов проверяемых файлов

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. Примеров множество: архивы, файлы, содержащие в себе макросы, таблицы, письма с вложениями и т.д.

Тип файлов для анализа на вирусы определяется в разделе **Типы файлов** (см. рис. 18). Выберите один из трех вариантов:

- **Проверять все файлы.** В данном случае будут подвергаться анализу все без исключения открываемые, запускаемые и сохраняемые объекты файловой системы.
- **Проверять программы и документы (по содержимому).** При выборе такой группы файлов Файловый Антивирус будет проверять только по-

тенциально заражаемые файлы – файлы, в которые может внедриться вирус.

Информация.

Существует ряд файловых форматов, вероятность внедрения в которые вредоносного кода и его последующая активация достаточно низка. Примером такого файла является файл *txt*-формата.

И наоборот, есть файловые форматы, которые содержат или могут содержать исполняемый код. Примером таких объектов являются файлы форматов *exe*, *dll*, *doc*. Риск внедрения и активации в такие файлы вредоносного кода достаточно высок.

Прежде чем приступать к поиску вирусов в файле, выполняется анализ его внутреннего заголовка на предмет формата файла (*txt*, *doc*, *exe* и т.д.). Если в результате анализа выясняется, что файл такого формата незаражаем, он не проверяется на присутствие вирусов и сразу же становится доступным для работы. Если же формат файла предполагает возможность внедрения вирусов, файл проверяется на вирусы.

- **Проверять программы и документы (по расширению).** В этом случае Файловый Антивирус будет проверять только потенциально заражаемые файлы, но формат файла будет определяться на основании его расширения. Воспользовавшись ссылкой [расширению](#), вы можете ознакомиться со списком расширений файлов (см. п. А.1 на стр. 232), которые подвергаются проверке в данном случае.

Совет.

Не стоит забывать, что злоумышленник может отправить вирус на ваш компьютер в файле с расширением *txt*, хотя на самом деле он может быть исполняемым файлом, переименованным в *txt*-файл. Если вы выберете вариант ● **Проверять программы и документы (по расширению)**, то такой файл будет пропущен в процессе проверки. Если же выбран вариант ● **Проверять программы и документы (по содержимому)**, невзирая на расширение, Файловый Антивирус проанализирует заголовок файла, в результате чего выяснится, что файл имеет *exe*-формат. Такой файл будет подвергнут тщательной проверке на вирусы.

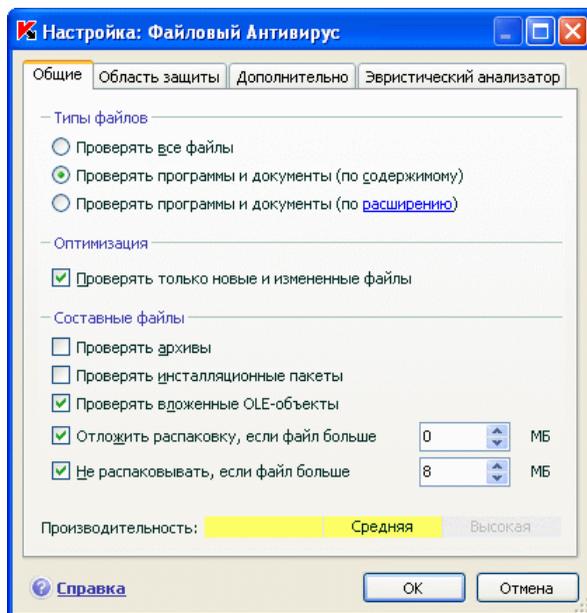


Рисунок 18. Выбор типов файлов, подвергаемых антивирусной проверке

В разделе **Оптимизация** можно сделать оговорку, что проверять на вирусы следует только новые файлы и те, что изменились с момента предыдущего их анализа. Такой режим работы позволяет заметно сократить время проверки и увеличить скорость работы приложения. Для этого необходимо установить флажок **Проверять только новые и измененные файлы**. Этот режим работы распространяется как на простые, так и на составные файлы.

В разделе **Составные файлы** укажите, какие составные файлы необходимо анализировать на присутствие вирусов:

- Проверять **все/только новые** архивы – проверять архивы форматов ZIP, CAB, RAR, ARJ.
- Проверять **все /только новые** установочные пакеты – анализировать на присутствие вирусов самораспаковывающиеся архивы.
- Проверять **все /только новые** вложенные OLE-объекты – проверять встроенные в файл объекты (например, Excel-таблица или макрос, внедренный в файл Microsoft Word, вложение почтового сообщения и т.д.).

Для каждого типа составного файла вы можете выбрать, проверять все файлы или только новые. Для этого воспользуйтесь ссылкой рядом с названием объекта. Она меняет свое значение при щелчке по ней левой кла-

вишей мыши. Если в разделе **Оптимизация** установлен режим проверки только новых и измененных файлов, выбор типа проверяемых составных файлов будет недоступен.

Чтобы указать, какие составные файлы не стоит проверять на вирусы, воспользуйтесь следующими параметрами:

- Отложить распаковку, если файл больше ... МБ.** В случае, если размер составного объекта превышает данное ограничение, он будет проверен приложением как единый объект (проанализирован заголовок) и предоставлен пользователю для работы. Проверка объектов, входящих в его состав, будет произведена позже. Если флажок не установлен, доступ к файлам больше указанного размера блокируется до завершения проверки объектов.
- Не распаковывать, если файл больше ... МБ.** В этом случае файл больше указанного размера будет пропущен без антивирусной проверки.

7.2.2. Формирование области защиты

Файловый Антивирус по умолчанию проверяет все файлы в момент обращения к ним, независимо от того, на каком носителе они расположены, будь то жесткий диск, CD/DVD-ROM или флеш-карта.

Вы можете ограничить область защиты. Для этого:

1. Откройте окно настройки приложения и выберите компонент **Файловый Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 17).
3. В открывшемся окне выберите закладку **Область защиты** (см. рис. 19).

На закладке представлен список объектов, которые будут подвергаться проверке Файловым Антивирусом. По умолчанию включена защита всех объектов, расположенных на жестких, сменных и сетевых дисках, подключенных к вашему компьютеру. Вы можете наполнить или отредактировать список с помощью кнопок **Добавить**, **Изменить**, **Удалить**.

Если вы хотите сузить круг защищаемых объектов, вы можете сделать это следующими способами:

1. Указать только те каталоги, диски или файлы, которые нужно защищать.
2. Сформировать список объектов, которые защищать не нужно.

3. Объединить первый и второй способы, то есть сформировать область защиты, из которой исключить ряд объектов.

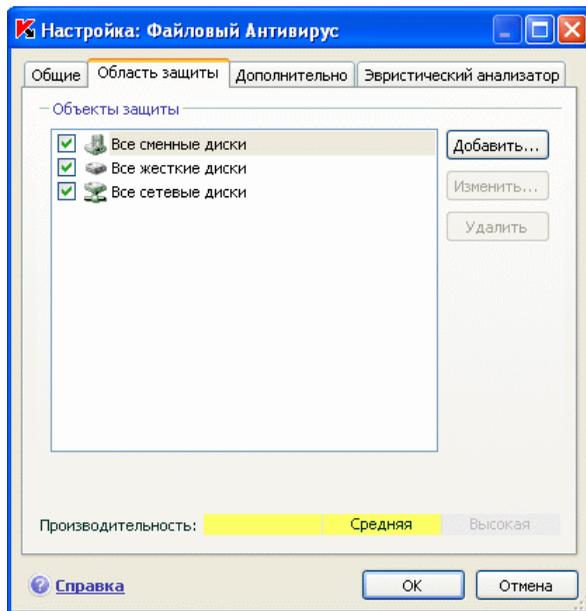


Рисунок 19. Формирование защищаемой области

При добавлении объекта для проверки возможно использование масок. Обратите внимание, что допускается ввод масок только с абсолютными путями к объектам:

- **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 один символ
- **C:\dir\test** – только файл *C:\dir\test*

Чтобы проверка выбранного объекта выполнялась рекурсивно, установите флажок **Включая вложенные папки**.

Внимание.

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 вашего компьютера!

7.2.3. Настройка дополнительных параметров

В качестве дополнительных параметров Файлового Антивируса вы можете указать режим проверки объектов файловой системы, а также настроить условия временной остановки работы компонента.

Для настройки дополнительных параметров Файлового Антивируса:

1. Откройте окно настройки приложения и выберите компонент **Файловый Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 17).
3. В открывшемся окне выберите закладку **Дополнительно** (см. рис. 20).

Режимом проверки объектов определяются условия срабатывания Файлового Антивируса. Возможны следующие варианты:

- **Интеллектуальный режим.** Данный режим направлен на повышение скорости обработки объектов и предоставления их пользователю для работы. При его выборе решение о проверке принимается на основании анализа операций, выполняемых с объектом.

Например, при работе с документом Microsoft Office Антивирус Касперского проверяет файл при первом открытии и последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

Интеллектуальный режим проверки объектов используется по умолчанию.

- **При открытии и изменении** – проверять объекты Файловым Антивирусом при открытии и изменении.
- **При открытии** – проверять объекты только при попытке открытия.
- **При выполнении** – проверять объекты только в момент попытки запуска.

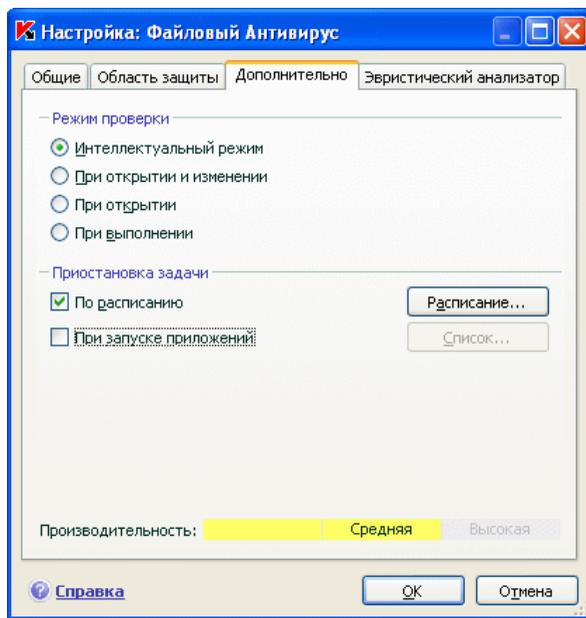


Рисунок 20. Настройка дополнительных параметров Файлового Антивируса

Временная остановка Файлового Антивируса может потребоваться при выполнении работ, требующих значительных ресурсов операционной системы. Для того чтобы снизить нагрузку и обеспечить быстрый доступ пользователя к объектам, рекомендуется настроить отключение компонента в определенное время либо при работе с определенными программами.

Для того чтобы остановить работу компонента на некоторое время, установите флажок **По расписанию** и в окне (см. рис. 20), открываемом по кнопке **Расписание**, задайте временные рамки отключения и возобновления работы компонента. Для этого введите значения в формате ЧЧ:ММ в соответствующих полях.

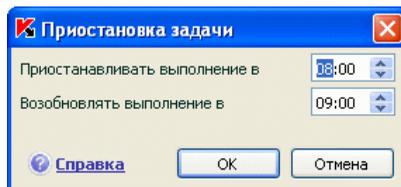


Рисунок 21. Приостановка работы компонента

Для отключения работы компонента при работе с программами, требующими значительных ресурсов, установите флажок **При запуске приложе-**

ний и в окне (см. рис. 22), открываемом по кнопке **Список**, сформируйте список программ.

Для добавления приложения в список воспользуйтесь кнопкой **Добавить**. Будет открыто контекстное меню, в котором из пункта **Обзор** вы можете перейти в стандартное окно выбора файлов и указать исполняемый файл добавляемого приложения. Либо из пункта **Приложения** перейти к списку приложений, работающих в данный момент, и выбрать нужное.

Для удаления приложения выберите его в списке и нажмите на кнопку **Удалить**.

Вы можете временно отключать остановку Файлового Антивируса при работе конкретного приложения. Для этого достаточно снять флажок напротив имени приложения, не удаляя его из списка.

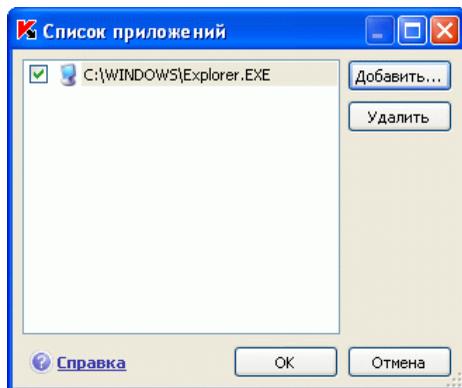


Рисунок 22. Формирование списка приложений

7.2.4. Использование методов эвристического анализа

Методы эвристического анализа используются в работе некоторых компонентов постоянной защиты, например, Файлового, Почтового и Веб-Антивирусов, а также задач поиска вирусов.

Известно, что проверка на основе сигнатурного метода с использованием сформированных заранее баз, содержащих описание известных угроз и методов их лечения, дает однозначный ответ, является ли проверяемый объект вредоносным, а также к какому классу опасных программ он относится. Эвристический метод, в отличие от сигнатурного метода, нацелен на обнаружение не сигнатур вредоносного кода, а типичных последовательностей операций, позволяющих сделать вывод о природе файла с достаточной долей вероятности. Преимуществом эвристического анализа является

то, что для его работы не требуется наличие предварительно составленных баз. За счет этого новые угрозы распознаются до того, как их активность становится известна вирусным аналитикам.

При подозрении на угрозу эвристический анализатор эмулирует выполнение объекта в безопасном виртуальном окружении Антивируса Касперского. В случае если при его выполнении будут обнаружены подозрительные действия, объект будет признан вредоносным и его запуск на компьютере будет заблокирован либо на экран будет выведено уведомление с запросом дальнейших действий у пользователя:

- 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.

Для использования методов эвристики установите флажок  **Использовать эвристический анализатор**. Дополнительно вы можете выбрать уровень детализации проверки, для этого передвиньте бегунок в одну из позиций: **поверхностный**, **средний** или **детальный**. Уровень детализации проверки обеспечивает баланс между тщательностью, а, значит, и качеством, поиска новых угроз и степенью загрузки ресурсов операционной системы, а также временем проверки. Чем выше установлен уровень эвристики, тем больше ресурсов системы требует проверка, и тем дольше по времени она выполняется.

Внимание!

Новые угрозы, обнаруживаемые с помощью эвристического анализа, оперативно анализируются специалистами «Лаборатории Касперского» и методы их лечения заносятся в ежечасно обновляемые базы приложения.

Поэтому, если вы регулярно выполняете обновление баз приложения и поддерживаете оптимальный уровень защиты компьютера, нет необходимости использовать методы эвристического анализа постоянно.

На закладке **Эвристический анализатор** (см. рис. 23) вы можете включать/отключать использование эвристических методов обнаружения новых угроз в рамках работы компонента Файловый Антивирус. Для этого выполните следующие действия:

1. Откройте окно настройки приложения и выберите компонент **Файловый Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 17).

3. В открывшемся окне выберите закладку **Эвристический анализатор**.

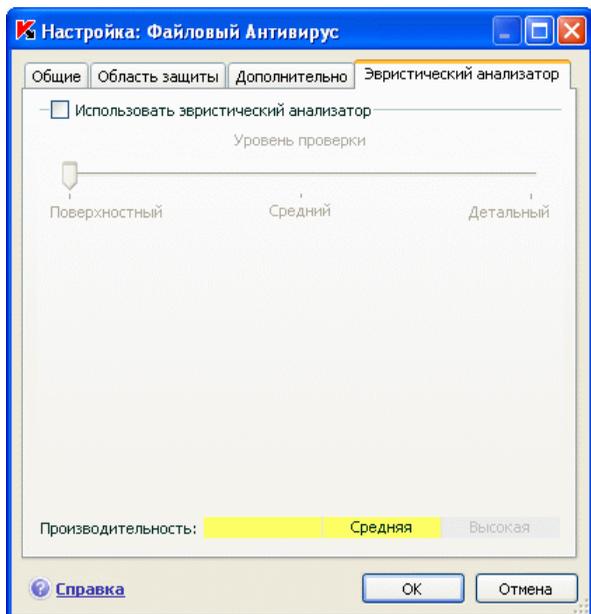


Рисунок 23. Использование методов эвристического анализа

7.2.5. Восстановление параметров защиты файлов 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.

Чтобы восстановить параметры защиты файлов по умолчанию,

1. Откройте окно настройки приложения и выберите компонент **Файловый Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **По умолчанию** в блоке **Уровень безопасности** (см. рис. 17).

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. Для сохранения списка объектов в открывшемся окне **Восстановление параметров** установите флажок **Область защиты**.

7.2.6. Выбор действия над объектами

Если в результате проверки файла на вирусы выясняется, что он заражен или подозревается на заражение, дальнейшие операции Файлового Антивируса зависят от статуса объекта и выбранного действия.

Файловый Антивирус может присвоить объекту один из следующих статусов:

- статус одной из вредоносных программ (например, *вирус, троянская программа*) (см. п. 1.3 на стр. 12).
- *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.

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

Чтобы изменить действие над объектом,

откройте окно настройки приложения и выберите компонент **Файловый Антивирус** в разделе **Защита**. Все возможные действия приведены в соответствующем разделе (см. рис. 24).

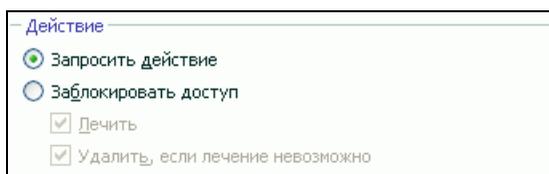


Рисунок 24. Возможные действия Файлового Антивируса над опасным объектом

Если в качестве действия вы выбрали	При обнаружении опасного объекта
 Запросить действие	Файловый Антивирус выдает на экран предупреждающее сообщение, содержащее информацию о том, каким вредоносным объектом заражен / возможно заражен файл, и

Если в качестве действия вы выбрали	При обнаружении опасного объекта
	предлагает на выбор одно из дальнейших действий. В зависимости от статуса объекта действия могут быть разными.
<input type="radio"/> Заблокировать доступ	Файловый Антивирус блокирует доступ к объекту. Информация об этом фиксируется в отчете (см. п. 15.3 на стр. 177). Позже можно попытаться вылечить этот объект.
<input type="radio"/> Заблокировать доступ <input checked="" type="checkbox"/> Лечить	Файловый Антивирус блокирует доступ к объекту и пытается его лечить. Если удалось вылечить объект, он предоставляется для работы. Если объект не удалось вылечить, то ему присваивается статус <i>возможно зараженный</i> , и он помещается на карантин (см. п. 15.1 на стр. 171). Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.
<input type="radio"/> Заблокировать доступ <input checked="" type="checkbox"/> Лечить <input checked="" type="checkbox"/> Удалить, если лечение невозможно	Файловый Антивирус блокирует доступ к объекту и пытается его лечить. Если удалось вылечить объект, он предоставляется для работы. Если объект не удалось вылечить, он удаляется. При этом копия объекта сохраняется в резервном хранилище (см. п. 15.2 на стр. 175).
<input type="radio"/> Заблокировать доступ <input checked="" type="checkbox"/> Удалить	Файловый Антивирус блокирует доступ к объекту и удаляет его.

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.

7.3. Отложенное лечение объектов

Если в качестве действия над вредоносными объектами вы выбрали  **Заблокировать доступ**, то объекты не будут подвергнуты лечению, и доступ к ним будет закрыт.

Если в качестве действия выбрано

 **Заблокировать доступ**

Лечить

то все невылеченные объекты также будут заблокированы.

Чтобы вновь получить доступ к заблокированным объектам, вам нужно предварительно полечить их. Для этого:

1. Выберите компонент **Файловый Антивирус** в разделе **Защит** главного окна приложения и воспользуйтесь ссылкой Открыть отчет.
2. Выберите интересующие вас объекты на закладке **Обнаружено** и нажмите на кнопку **Действия** → **Лечить все**.

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 вашего компьютера. Настоятельно не рекомендуется пропускать вредоносные объекты.

ГЛАВА 8. АНТИВИРУСНАЯ ЗАЩИТА ПОЧТЫ

В состав Антивируса Касперского включен специальный компонент, обеспечивающий защиту входящей и исходящей почты на наличие опасных объектов, – *Почтовый Антивирус*. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все почтовые сообщения по протоколам POP3, SMTP, IMAP, MAPI¹ и NNTP, а также через защищенные соединения (SSL) по протоколам POP3 и IMAP.

Индикатором работы компонента является значок Антивируса Касперского в системной панели, который принимает вид  каждый раз при проверке письма.

По умолчанию защита почты осуществляется по следующему алгоритму:

1. Каждое письмо, принимаемое или отправляемое пользователем, перехватывается Почтовым Антивирусом.
2. Почтовое сообщение разбирается на составляющие его части: заголовков письма, тело, вложения.
3. Тело и вложения почтового сообщения (в том числе вложенные OLE-объекты) проверяются на присутствие в нем опасных объектов. Распознавание вредоносных объектов происходит на основании баз, используемых в работе приложения, и с помощью эвристического алгоритма. Базы содержат описание всех известных на настоящий момент вредоносных программ и способов их обезвреживания. Эвристический алгоритм позволяет обнаруживать новые вирусы, еще не описанные в базах.
4. В результате проверки на вирусы возможны следующие варианты поведения:
 - Если тело или вложение письма содержит вредоносный код, Почтовый Антивирус блокирует письмо, помещает копию зараженного объекта в *резервное хранилище* и пытается обезвредить объект. В результате успешного лечения письмо становится доступным для пользователя, если же лечение произвести не удалось, зараженный объект из

¹ Проверка почты по MAPI-протоколу выполняется с помощью специального модуля расширения в Microsoft Office Outlook и The Bat!

письма удаляется. В результате антивирусной обработки в тему письма помещается специальный текст, уведомляющий о том, что письмо обработано Антивирусом Касперского.

- Если тело или вложение письма содержит код, похожий на вредоносный, но стопроцентной гарантии этого нет, подозрительная часть письма помещается в специальное хранилище – *карантин*.
- Если в письме не обнаружено вредоносного кода, оно сразу же становится доступным для пользователя.

Для почтовой программы Microsoft Office Outlook предусмотрен специальный встраиваемый модуль расширения (см. п. 8.2.2 на стр. 102), позволяющий производить более тонкую настройку проверки почты.

Если вы используете почтовую программу The Bat!, Антивирус Касперского может использоваться наряду с другими антивирусными приложениями. При этом правила обработки почтового трафика (см. п. 8.2.3 на стр. 103) настраиваются непосредственно в программе The Bat! и превалируют над параметрами защиты почты Антивируса Касперского.

Внимание!

В данной версии Антивируса Касперского не предусмотрены модули расширения Почтового Антивируса для 64-разрядных версий почтовых клиентов.

При работе с остальными почтовыми программами (в том числе Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail) Почтовый Антивирус проверяет почту на трафике по протоколам SMTP, POP3, IMAP и NNTP.

Обратите внимание, что при работе в почтовом клиенте Thunderbird не проверяются на вирусы почтовые сообщения по протоколу IMAP, если используются фильтры, перемещающие сообщения из папки **Входящие**.

8.1. Выбор уровня безопасности почты

Антивирус Касперского обеспечивает защиту вашей почты на одном из следующих уровней (см. рис. 30):

Максимальная защита – уровень, на котором осуществляется максимально полный контроль за входящими и исходящими почтовыми

сообщениями. Приложение детально проверяет вложенные объекты писем, независимо от времени проверки, в том числе и архивы.

Рекомендуемый. Параметры данного уровня рекомендованы экспертами «Лаборатории Касперского». Они определяют проверку тех же объектов, что и на уровне **Максимальная защита**, за исключением вложенных объектов или писем, проверка которых занимает больше трех минут.

Максимальная скорость – уровень безопасности, позволяющий вам комфортно работать с приложениями, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых объектов почтовых сообщений на данном уровне сокращен. Так, на этом уровне проверяется только ваша входящая почта, причем не проверяются вложенные архивы и объекты (письма), проверка которых занимает более трех минут. Рекомендуется использовать этот уровень, если на вашем компьютере установлены дополнительные средства защиты почты.

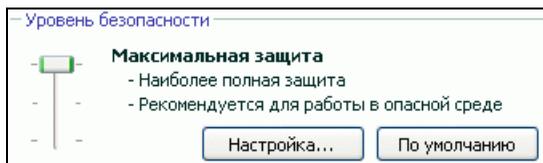


Рисунок 25. Выбор уровня безопасности почты

По умолчанию безопасность почты обеспечивается на **Рекомендуемом** уровне.

Вы можете повысить или понизить степень защиты вашей почты, выбрав соответствующий уровень или изменив параметры текущего уровня.

Для того чтобы изменить уровень безопасности,

переместите ползунок по шкале. Регулируя уровень безопасности, вы определяете соотношение между скоростью выполнения проверки и количеством проверяемых объектов: чем меньше объектов почтовых сообщений подвергается анализу на присутствие опасных объектов, тем выше скорость проверки.

Если какой-либо предустановленный уровень не полностью соответствует вашим требованиям, вы можете выполнить дополнительную настройку его параметров. Для этого рекомендуется выбрать наиболее близкий к вашим пожеланиям уровень в качестве базового и отредактировать его параметры. В этом случае название уровня безопасности будет изменено на **Другой**. Рассмотрим пример, когда может пригодиться изменение параметров предустановленных уровней безопасности.

Пример:

Ваш компьютер находится вне локальной сети и использует соединение с интернетом по модему. В качестве почтового клиента для получения и отправки электронной корреспонденции вы используете Microsoft Outlook Express, а в качестве почтовой службы – один из бесплатных почтовых сервисов. Ваша почта в силу ряда причин часто содержит вложенные архивы. Как максимально защитить ваш компьютер от заражения через электронную почту?

Совет по выбору уровня:

Анализируя исходные данные можно прийти к выводу, что опасность заражения вредоносной программой через электронную почту в приведенном примере чрезвычайно высока (отсутствие централизованной защиты почты и способ подключения к интернету).

В качестве базового предустановленного уровня безопасности рекомендуется использовать уровень **Максимальная защита** со следующими изменениями: рекомендуется сократить время проверки вложенных объектов, например, до 1-2 минут. Большинство вложенных архивов будут проверяться на вирусы и скорость обработки почты не будет сильно замедленной.

Чтобы изменить параметры текущего уровня безопасности,

1. Откройте окно настройки приложения и выберите компонент **Почтовый Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 25).
3. В открывшемся окне отредактируйте параметры защиты почты и нажмите на кнопку **ОК**.

8.2. Настройка защиты почты

Правила, по которым осуществляется проверка вашей почты, определяются набором параметров. Их можно разбить на следующие группы:

- параметры, определяющие защищаемый поток сообщений (см. п. 8.2.1 на стр. 100);
- параметры, определяющие использование методов эвристического анализа (см. п. 8.2.4 на стр. 105);
- параметры проверки почтовых сообщений в Microsoft Office Outlook (см. п. 8.2.2 на стр. 102) и The Bat! (см. п. 8.2.3 на стр. 103);
- параметры, определяющие действия над опасными объектами почтовых сообщений (см. п. 8.2.4 на стр. 105).

В данном разделе Руководства будут детально рассмотрены все перечисленные выше параметры.

8.2.1. Выбор защищаемого потока сообщений

Почтовый Антивирус позволяет вам выбрать, какой именно поток почтовых сообщений нужно проверять на присутствие опасных объектов.

По умолчанию компонент защищает почту в соответствии с параметрами **Рекомендуемого** уровня защиты, что означает проверку как входящих сообщений, так и исходящей почты. В самом начале работы с приложением рекомендуется проверять исходящую почту, поскольку существует вероятность того, что на вашем компьютере есть почтовые черви, которые используют электронную почту в качестве канала собственного распространения. Это позволит избежать неприятностей, связанных с неконтролируемой рассылкой зараженных электронных сообщений с вашего компьютера.

Если вы уверены в том, что письма, которые вы отправляете, не могут содержать опасных объектов, вы можете отключить проверку исходящей почты. Для этого:

1. Откройте окно настройки приложения и выберите компонент **Почтовый Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 25).
3. В открывшемся окне (см. рис. 26) выберите вариант **Только входящие сообщения** в блоке **Область защиты**.

Помимо выбора почтового потока вы можете уточнить, нужно ли контролировать вложенные в письма архивы, а также определить максимальное время проверки одного объекта письма. Эти параметры настраиваются в блоке **Оптимизация**.

Если ваш компьютер не защищен какими-либо средствами локальной сети, выход в интернет осуществляется без участия прокси-сервера или сетевого экрана, рекомендуется не отключать проверку вложенных архивов и не вводить ограничение времени проверки объектов.

Если же вы работаете в защищенном окружении, для увеличения скорости проверки почты возможно изменение временного ограничения на проверку объектов.

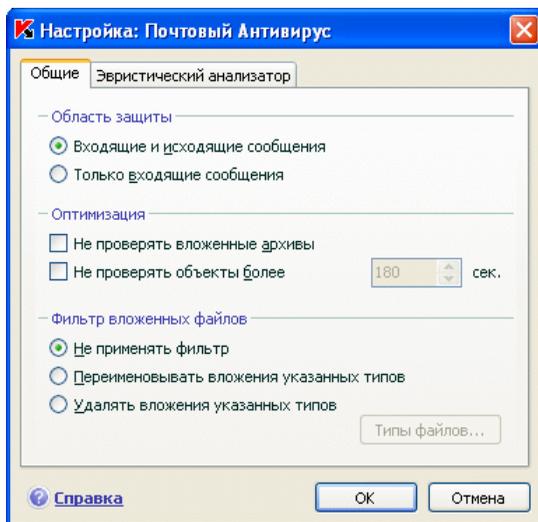


Рисунок 26. Настройка защиты почтового трафика

В блоке **Фильтр вложенных файлов** вы можете настроить условия фильтрации присоединенных к почтовому сообщению объектов:

- Не применять фильтр** – не использовать дополнительную фильтрацию присоединенных файлов.
- Переименовывать вложения указанных типов** – отфильтровывать вложенные файлы определенного формата и заменять последний символ имени файла на символ «подчеркивание». Выбрать тип файла можно в окне, открываемом по кнопке **Типы файлов**.
- Удалять вложения указанных типов** – отфильтровывать и удалять вложенные файлы определенного формата. Выбрать тип файла можно в окне, открываемом по кнопке **Типы файлов**.

Подробнее о типах файлов вложений, подвергаемых фильтрации, вы можете прочесть в разделе А.1 на стр. 232.

Использование фильтра обеспечит дополнительную безопасность вашему компьютеру, поскольку вредоносные программы распространяются через почту чаще всего в виде вложенных файлов. Переименование или удаление вложений определенного типа позволит защитить ваш компьютер от, например, автоматического запуска вложенного файла при получении сообщения.

8.2.2. Настройка проверки почты в Microsoft Office Outlook

Если в качестве почтового клиента вы используете Microsoft Office Outlook, вы можете дополнительно настроить проверку вашей почты на вирусы.

При установке Антивируса Касперского в Microsoft Office Outlook встраивается специальный модуль расширения. Он позволяет вам быстро перейти к настройке параметров Почтового Антивируса, а также определить, в какой момент времени почтовое сообщение будет проверено на присутствие опасных объектов.

Внимание!

В данной версии Антивируса Касперского не предусмотрен модуль расширения Почтового Антивируса для 64-разрядной Microsoft Office Outlook.

Модуль расширения реализован в качестве специальной закладки **Почтовый Антивирус**, расположенной в меню **Сервис** → **Параметры** (см. рис. 27).

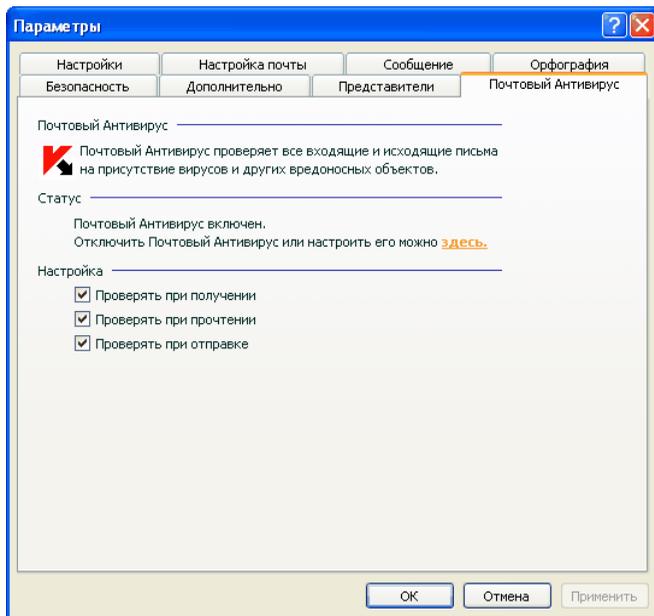


Рисунок 27. Детальная настройка защиты почты в Microsoft Office Outlook

Выберите режимы проверки почты:

- Проверять при получении** – анализировать каждое почтовое сообщение в момент его поступления в ваш почтовый ящик.
- Проверять при прочтении** – проверять письмо в тот момент, когда вы его открываете на чтение.
- Проверять при отправке** – анализировать каждое отправляемое вами почтовое сообщение на присутствие вирусов в момент его отправки.

Внимание!

Если вы используете подключение Microsoft Office Outlook к почтовому серверу по протоколу IMAP, рекомендуется не использовать режим **Проверять при получении**. Включение этого режима приводит к принудительному копированию письма на локальный компьютер в момент его доставки на сервер, вследствие чего теряется основное преимущество протокола IMAP – экономия трафика и управление нежелательными письмами на сервере без копирования на компьютер пользователя.

Действие, которое будет производиться над опасным объектом письма, определяется в параметрах Почтового Антивируса, перейти к настройке которых вы можете по ссылке [здесь](#).

8.2.3. Настройка проверки почты в The Bat!

Действия над зараженными объектами почтовых сообщений в почтовой программе The Bat! определяются средствами самой программы.

Внимание!

Параметры Почтового Антивируса, определяющие проверять или нет входящую и исходящую почту, а также действия над опасными объектами писем и исключения игнорируются. Единственное, что принимается во внимание программой The Bat!, – это проверка вложенных архивов и ограничение по времени проверки одного объекта письма (см. п. 8.2.1 на стр. 100).

В данной версии Антивируса Касперского не предусмотрен модуль расширения Почтового Антивируса для 64-разрядной версии The Bat!

Для того чтобы перейти к настройке параметров защиты почты в The Bat!,

1. В меню **Свойства** почтового клиента выберите пункт **Настройка**.

2. В дереве настройки выберите пункт **Защита от вирусов**.

Представленные параметры защиты (см. рис. 28) распространяются на все установленные на компьютере антивирусные модули, поддерживающие работу с The Bat!

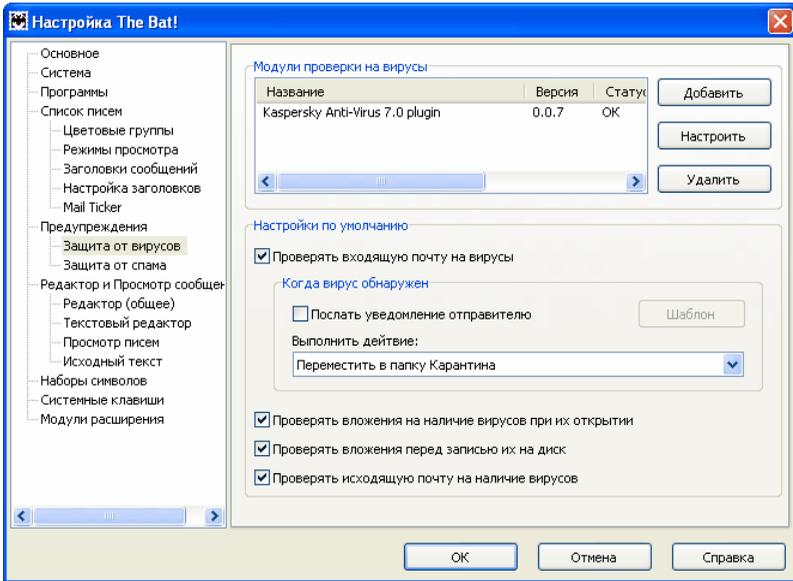


Рисунок 28. Настройка проверки почты в The Bat!

Вам нужно определить:

- какой поток почтовых сообщений подвергать антивирусной проверке (входящий, исходящий);
- в какой момент времени будет производиться проверка объектов письма на вирусы (при открытии письма, перед сохранением на диск);
- действия, предпринимаемые почтовым клиентом при обнаружении опасных объектов в почтовых сообщениях. Например, вы можете выбрать:

Попробовать излечить зараженные части – пытаться вылечить зараженный объект письма; если его вылечить невозможно, объект остается в письме. Антивирус Касперского обязательно уведомит вас о том, что объект почтового сообщения заражен. Но даже если вы выберете действие **Удалить** в окне уведомления Почтового Антивируса, объект останется в почтовом со-

общении, поскольку действие над объектом, выбранное в The Bat!, превалирует над действием Почтового Антивируса.

Удалить зараженные части – удалить опасный объект письма, независимо от того, является он зараженным или подозревается на заражение.

По умолчанию все зараженные объекты почтовых сообщений помещаются программой The Bat! в папку карантина без лечения.

Внимание!

Почтовые сообщения, содержащие опасные объекты, не отмечаются специальным заголовком в программе The Bat!

8.2.4. Использование методов эвристического анализа

Методы эвристического анализа используются в работе некоторых компонентов постоянной защиты, а также задач поиска вирусов (подробнее см. см. п. 7.2.4 на стр. 90).

Вы можете включать/ отключать использование эвристических методов обнаружения новых угроз в рамках работы компонента Почтовый Антивирус. Для этого выполните следующие действия:

1. Откройте окно настройки приложения и выберите компонент **Почтовый Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 25)
3. В открывшемся окне выберите закладку **Эвристический анализатор** (см. рис. 29).

Для использования методов эвристики установите флажок **Использовать эвристический анализатор**. Дополнительно вы можете выбрать уровень детализации проверки, для этого передвиньте бегунок в одну из позиций: **поверхностный**, **средний** или **детальный**.

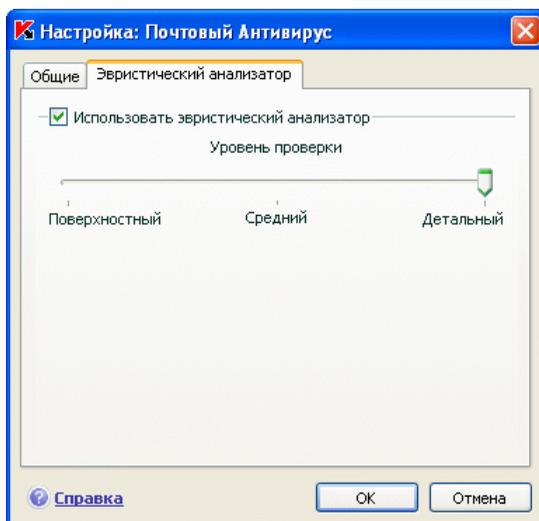


Рисунок 29. Использование методов эвристического анализа

8.2.5. Восстановление параметров защиты почты по умолчанию

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

Чтобы восстановить параметры защиты почты по умолчанию,

1. Откройте окно настройки приложения и выберите компонент **Почтовый Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **По умолчанию** в блоке **Уровень безопасности** (см. рис. 25).

8.2.6. Выбор действия над опасным объектом письма

Если в результате проверки почтового сообщения на вирусы выясняется, что письмо или какой-либо его объект (тело, вложение) заражен или подозревается на заражение, дальнейшие операции Почтового Антивируса зависят от статуса объекта и выбранного действия.

Объекту письма в результате проверки может быть присвоен один из следующих статусов:

- статус одной из вредоносных программ (например, *вирус*, *троянская программа*, подробнее см. п. 1.3 на стр. 12);
- *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.

По умолчанию при обнаружении опасного или возможно зараженного объекта Почтовый Антивирус выдает на экран предупреждение и предлагает на выбор несколько действий над объектом.

Чтобы изменить действие над объектом,

откройте окно настройки приложения и выберите компонент **Почтовый Антивирус** в разделе **Защита**. Все возможные действия над опасными объектами приведены в блоке **Действие** (см. рис. 30).

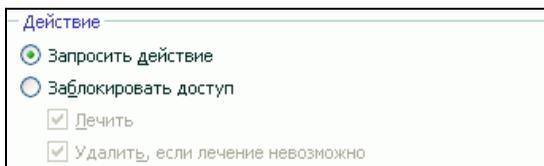


Рисунок 30. Выбор действия над опасным объектом письма

Рассмотрим подробнее возможные варианты обработки опасных объектов почтовых сообщений.

Если в качестве действия вы выбрали	При обнаружении опасного объекта
<input checked="" type="radio"/> Запросить действие	Почтовый Антивирус выдаст на экран предупреждающее сообщение, содержащее информацию о том, каким вредоносным объектом заражен (возможно заражен) объект, и предложит на выбор одно из дальнейших действий.
<input checked="" type="radio"/> Заблокировать доступ	Почтовый Антивирус блокирует доступ к объекту. Информация об этом фиксируется в отчете (см. п. 15.3 на стр. 177). Позже можно попытаться вылечить этот объект.

Если в качестве действия вы выбрали	При обнаружении опасного объекта
<input checked="" type="radio"/> Заблокировать доступ <input checked="" type="checkbox"/> Лечить	Почтовый Антивирус блокирует доступ к объекту и пытается его лечить. Если удалось вылечить объект, он предоставляется 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="radio"/> Заблокировать доступ <input checked="" type="checkbox"/> Лечить <input checked="" type="checkbox"/> Удалить, если лечение невозможно²	Почтовый Антивирус блокирует доступ к объекту и пытается его лечить. Если удалось вылечить объект, он предоставляется для работы. Если объект не удалось вылечить, он удаляется. При этом копия объекта сохраняется в резервном хранилище. Объект со статусом <i>возможно заражен</i> будет помещен на карантин.
<input checked="" type="radio"/> Заблокировать доступ <input checked="" type="checkbox"/> Удалить	Почтовый Антивирус блокирует доступ к объекту (зараженному или возможно зараженному) и удалит его.

Перед лечением или удалением объекта Антивирус Касперского формирует его резервную копию и помещает ее в резервное хранилище (см. п. 15.2 на стр. 175) на тот случай, если понадобится восстановить объект или появится возможность его вылечить.

² Если в качестве почтовой программы используется The Bat!, то при таком действии Почтового Антивируса опасные объекты писем будут либо лечиться, либо удаляться (в зависимости от того, какое действие выбрано в The Bat!).

ГЛАВА 9. ВЕБ-ЗАЩИТА

Каждый раз при работе в интернете вы подвергаете информацию, хранящуюся на вашем компьютере, риску заражения опасными программами. Они могут проникнуть на ваш компьютер, пока вы просматриваете некоторую статью в интернете.

Для обеспечения безопасности вашей работы в интернете Антивирус Касперского включает специальный компонент – *Веб-Антивирус*. Он защищает информацию, поступающую на ваш компьютер по HTTP-протоколу, а также предотвращает запуск на компьютере опасных скриптов.

Внимание!

Веб-защита предусматривает контроль HTTP-трафика, проходящего только через порты, указанные в списке контролируемых портов (см. п. 15.4 на стр. 185). Список портов, которые чаще всего используются для передачи почты и HTTP-трафика, включен в поставку приложения. Если вы используете порты, отсутствующие в данном списке, для обеспечения защиты проходящего через них трафика добавьте их в список.

Если вы работаете в незащищенном пространстве, рекомендуется использовать Веб-Антивирус для защиты вашей работы в интернете. Если же ваш компьютер работает в сети, защищенной сетевым экраном или фильтрами HTTP-трафика, Веб-Антивирус обеспечит дополнительную защиту работы в интернете.

Индикатором работы компонента является значок Антивируса Касперского в системной панели, который принимает вид  каждый раз при проверке скриптов.

Рассмотрим подробнее схему работы компонента.

Веб-Антивирус состоит из двух модулей, обеспечивающих:

- *Защиту HTTP-трафика* – проверку всех объектов, поступающих на компьютер пользователя по протоколу HTTP.
- *Проверку скриптов* – проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в интернете.

Для программы Microsoft Internet Explorer предусмотрен специальный модуль расширения, который встраивается в программу при установке Антивируса Касперского. О его наличии свидетельствует кнопка  в панели инструментов браузера. При нажатии на нее открыва-

ется информационная панель со статистикой Веб-Антивируса по количеству проверенных и заблокированных скриптов.

Защита HTTP-трафика обеспечивается по следующему алгоритму:

1. Каждая веб-страница или файл, к которому происходит обращение пользователя или некоторой программы по протоколу HTTP, перехватывается и анализируется Веб-Антивирусом на присутствие вредоносного кода. Распознавание вредоносных объектов происходит на основании баз, используемых в работе Антивируса Касперского, и с помощью эвристического алгоритма. Базы содержат описание всех известных на настоящий момент вредоносных программ и способов их обезвреживания. Эвристический алгоритм позволяет обнаруживать новые вирусы, еще не описанные в базах.
2. В результате анализа возможны следующие варианты поведения:
 - Если веб-страница или объект, к которому обращается пользователь, содержат вредоносный код, доступ к нему блокируется. При этом на экран выводится уведомление о том, что запрашиваемый объект или страница заражена.
 - Если файл или веб-страница не содержат вредоносного кода, они сразу же становятся доступны для пользователя.

Проверка скриптов выполняется по следующему алгоритму:

1. Каждый запускаемый на веб-странице скрипт перехватывается Веб-Антивирусом и анализируется на присутствие вредоносного кода.
2. Если скрипт содержит вредоносный код, Веб-Антивирус блокирует его, уведомляя пользователя специальным всплывающим сообщением.
3. Если в скрипте не обнаружено вредоносного кода, он выполняется.

9.1. Выбор уровня безопасности веб-защиты

Антивирус Касперского обеспечивает безопасность вашей работы в интернете на одном из следующих уровней (см. рис. 31):

Максимальная защита – уровень, на котором осуществляется максимально полный контроль за скриптами и объектами, поступающими по HTTP-протоколу. Приложение детально проверяет все объекты, используя полный набор баз приложения. Такой уровень безопасности рекомендуется использовать в агрессивном окружении, когда не используются другие средства защиты HTTP-трафика.

Рекомендуемый. Параметры данного уровня рекомендованы экспертами «Лаборатории Касперского». Они определяют проверку тех же объектов, что и на уровне **Максимальная защита**, однако ограничивают время кеширования фрагмента файла, что позволяет ускорить проверку и передачу объекта пользователю.

Максимальная скорость – уровень безопасности, позволяющий вам комфортно работать с приложениями, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых объектов на данном уровне сокращен за счет использования ограниченного набора баз приложений. Рекомендуется включать этот уровень безопасности, если на вашем компьютере установлены дополнительные средства веб-защиты.

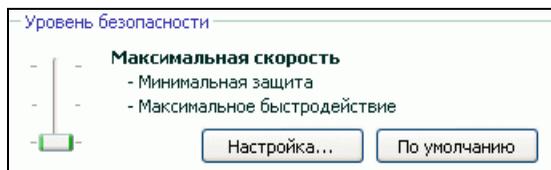


Рисунок 31. Выбор уровня веб-защиты

По умолчанию защита осуществляется на **Рекомендуемом** уровне.

Вы можете повысить или понизить степень защиты, выбрав соответствующий уровень или изменив параметры текущего уровня.

Для того чтобы изменить уровень безопасности,

переместите ползунок по шкале. Регулируя уровень безопасности, вы определяете соотношение между скоростью выполнения проверки и количеством проверяемых объектов: чем меньше объектов подвергается анализу на присутствие вредоносного кода, тем выше скорость проверки.

Если какой-либо предустановленный уровень не полностью соответствует вашим требованиям, вы можете выполнить дополнительную настройку его параметров. Для этого рекомендуется выбрать наиболее близкий к вашим пожеланиям уровень в качестве базового и отредактировать его параметры. В этом случае название уровня безопасности будет изменено на **Другой**. Рассмотрим пример, когда может пригодиться изменение параметров предустановленных уровней безопасности.

Пример:

Ваш компьютер соединяется с интернетом по модему. Он не включен в корпоративную локальную сеть, и антивирусная защита входящего трафика по HTTP-протоколу отсутствует.

Вы в силу особенностей своей работы часто скачиваете из интернета файлы большого объема. Проверка таких файлов, как правило, занимает достаточное количество времени.

Как максимально защитить ваш компьютер от заражения через HTTP-трафик или скрипт?

Совет по выбору уровня:

Анализируя исходные данные, можно прийти к выводу, что ваш компьютер работает в агрессивной среде и опасность заражения вредоносной программой через HTTP-трафик чрезвычайно высока (отсутствии централизованной веб-защиты и способ подключения к интернету).

В качестве базового предустановленного уровня безопасности рекомендуется использовать уровень **Максимальная защита** со следующими изменениями: рекомендуется настроить ограничение на время кеширования фрагментов файлов при проверке.

Чтобы изменить параметры предустановленного уровня безопасности,

1. Откройте окно настройки приложения и выберите компонент **Веб-Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 31).
3. В открывшемся окне отредактируйте параметры Веб-Антивируса и нажмите на кнопку **ОК**.

9.2. Настройка веб-защиты

Веб-защита обеспечивает проверку всех объектов, загружаемых на ваш компьютер по протоколу HTTP, и обеспечивает контроль за всеми запускаемыми WSH-скриптами (JavaScript, Visual Basic Script и др.).

Вы можете настроить ряд параметров Веб-Антивируса, направленных на повышение скорости работы компонента, а именно:

- определить алгоритм проверки, выбрав использование полного или ограниченного набора баз приложения (см. п. 9.2.1 на стр. 113);
- сформировать список адресов, содержанию которых вы доверяете (см. п. 9.2.3 на стр. 115);
- включить/ выключить использование методов эвристического анализа (см. п. 9.2.3 на стр. 115).

Помимо этого вы можете выбрать действие над опасным объектом HTTP-трафика, которое будет выполнять Веб-Антивирус.

В данном разделе Руководства будут детально рассмотрены все перечисленные выше параметры.

9.2.1. Определение алгоритма проверки

Проверка данных, поступающих из интернета, может осуществляться по одному из следующих алгоритмов:

- *Потоковая проверка* – технология обнаружения вредоносного кода в сетевом трафике, при которой поток данных проверяется «на лету». Например, вы скачиваете файл из интернета. Веб-Антивирус проверяет файл порциями по мере копирования данных на компьютер. Эта технология позволяет увеличить скорость доставки проверенного объекта пользователю. В то же время для реализации потоковой проверки используется сокращенный набор баз приложения (только наиболее активные угрозы), что значительно сокращает уровень безопасности вашей работы в интернете.
- *Проверка с буферизацией* – технология обнаружения вредоносного кода в сетевом трафике, при которой проверка объекта осуществляется после его полного копирования в буфер. После этого объект подвергается анализу на вирусы и по результатам анализа передается пользователю для работы либо блокируется.

При использовании данного типа проверки применяется полный набор баз приложения, что позволяет значительно повысить уровень обнаружения вредоносного кода. Однако использование этого алгоритма увеличивает время обработки объекта и передачи его пользователю для работы, а также может вызывать проблемы при копировании и обработке больших объектов, связанные с истечением тайм-аута на соединение HTTP-клиента.

Для решения этой проблемы мы предлагаем ввести ограничение на время кеширования фрагментов объекта, поступающего из интернета. При истечении этого ограничения каждая полученная часть файла будет передаваться пользователю непроверенной, а по завершении копирования объекта он будет проверен целиком. Это позволит уменьшить время передачи объекта пользователю, решить проблему разрыва соединения, не сокращая уровень безопасности работы в интернете.

Чтобы выбрать алгоритм проверки, который будет использоваться Веб-Антивирусом:

1. Откройте окно настройки приложения и выберите компонент **Веб-Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 31).

3. В открывшемся окне (см. рис. 32) выберите нужное значение в блоке **Алгоритм проверки**.

По умолчанию Веб-Антивирус проверяет данные из интернета с буферизацией, используя полный набор баз приложения. Также настроено ограничение на время кеширования фрагментов файла в 1 секунду.

Внимание!

Если при работе с такими ресурсами как интернет-радио, интернет-видео, интернет-конференции возникают проблемы с доступностью запрашиваемых объектов, используйте алгоритм потоковой проверки.

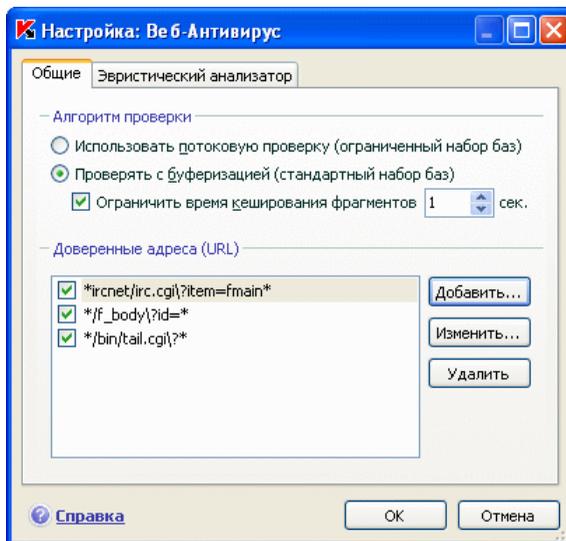


Рисунок 32. Настройка уровня веб-защиты

9.2.2. Формирование списка доверенных адресов

Вам предоставляется возможность сформировать список доверенных адресов, содержанию которых вы безоговорочно доверяете. Веб-Антивирус не будет анализировать информацию с данных адресов на присутствие опасных объектов. Такая возможность может быть использована в том случае, если Веб-Антивирус препятствует загрузке некоторого файла, блокируя попытки его скачать.

Чтобы сформировать список доверенных адресов,

1. Откройте окно настройки приложения и выберите компонент **Веб-Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 31).
3. В открывшемся окне (см. рис. 32) сформируйте список доверенных серверов в блоке **Доверенные адреса (URL)**. Для этого используйте кнопки, расположенные справа от списка.

При вводе доверенного адреса вы можете формировать маски, используя следующие специальные символы:

* – любая последовательность символов.

Пример: При вводе маски ***abc*** не будет проверяться любой URL-адрес, содержащий последовательность **abc**, например, www.virus.com/download_virus/page_0-9abcdef.html.

? – любой один символ.

Пример: При вводе маски **Patch_123?.com** не будет проверяться URL-адрес, содержащий заданную последовательность символов и любой символ, следующий за 3, например, **Patch_1234.com**. Однако адрес **patch_12345.com** будет проверяться.

В случае, если символы * и ? входят в состав реального URL-адреса, добавляемого в список, необходимо при их вводе использовать символ \ – отмена одного из следующих за ним символов *, ?, \.

Пример: в качестве доверенного адреса необходимо добавить следующий URL-адрес: www.virus.com/download_virus/virus.dll?virus_name=

Для того чтобы Антивирус Касперского не воспринял ? как символ исключения, нужно поставить перед ? знак \. В этом случае URL-адрес, добавляемый в список исключений, будет следующим: www.virus.com/download_virus/virus.dll?virus_name=

9.2.3. Использование методов эвристического анализа

Методы эвристического анализа используются в работе некоторых компонентов постоянной защиты, а также задач поиска вирусов (подробнее см. см. п. 7.2.4 на стр. 90).

Вы можете включать/ отключать использование эвристических методов обнаружения новых угроз в рамках работы компонента Веб-Антивирус. Для этого выполните следующие действия:

1. Откройте окно настройки приложения и выберите компонент **Веб-Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности**.
3. В открывшемся окне выберите закладку **Эвристический анализатор** (см. рис. 33).

Для использования методов эвристики установите флажок **Использовать эвристический анализатор**. Дополнительно вы можете выбрать уровень детализации проверки, для этого передвиньте бегунок в одну из позиций: **поверхностный**, **средний** или **детальный**.

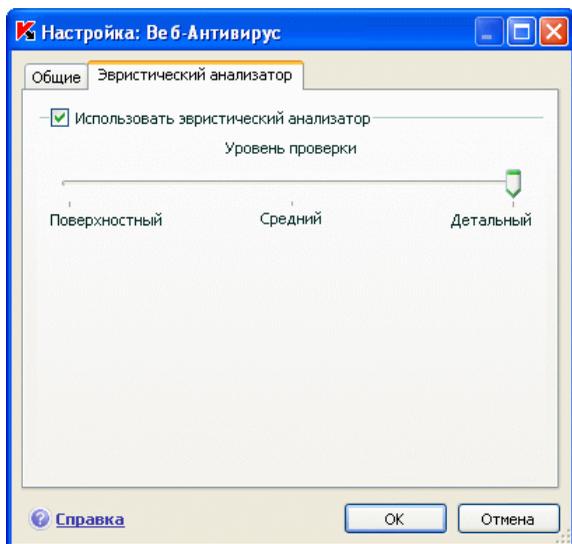


Рисунок 33. Использование методов эвристического анализа

9.2.4. Восстановление параметров веб-защиты по умолчанию

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

Чтобы восстановить параметры Веб-Антивируса по умолчанию,

1. Откройте окно настройки приложения и выберите компонент **Веб-Антивирус** в разделе **Защита**.
2. Нажмите на кнопку **По умолчанию** в блоке **Уровень безопасности** (см. рис. 31).

9.2.5. Выбор действия над опасным объектом

Если в результате анализа объекта HTTP-трафика выясняется, что он содержит вредоносный код, дальнейшие операции Веб-Антивируса зависят от указанного вами действия.

Чтобы настроить реакцию Веб-Антивируса при обнаружении опасного объекта:

откройте окно настройки приложения и выберите компонент **Веб-Антивирус** в разделе **Защита**. Все возможные действия над опасными объектами приведены в блоке **Действие** (см. рис. 34).

По умолчанию при обнаружении опасного объекта HTTP-трафика Веб-Антивирус выдает на экран предупреждение и предлагает на выбор несколько действий над объектом.



Рисунок 34. Выбор действия над опасным скриптом

Рассмотрим подробнее возможные варианты обработки опасных объектов HTTP-трафика.

Если в качестве действия вы выбрали	При обнаружении опасного объекта в HTTP-трафике
 Запросить действие	Веб-Антивирус выдаст на экран предупреждающее сообщение, содержащее информацию о том, каким вредоносным кодом заражен объект, и предложит на выбор одно из дальнейших действий.

 Заблокировать	Веб-Антивирус заблокирует доступ к объекту и выведет на экран окно уведомления о блокировке. Аналогичная информация будет зафиксирована в отчете (см. п. 15.3 на стр. 177).
 Разрешить	Веб-Антивирус разрешает доступ к опасному объекту. Информация об этом фиксируется в отчете.

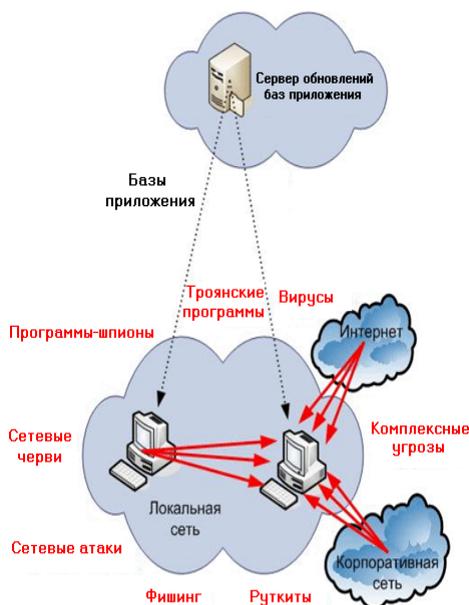
Что касается действий над опасными скриптами, то Веб-Антивирус всегда блокирует их исполнение и выводит на экран всплывающее сообщение, уведомляющее пользователя о выполненном действии. Вы не можете изменить действие над опасным скриптом, кроме как отключить работу модуля проверки скриптов.

ГЛАВА 10. ПРОАКТИВНАЯ ЗАЩИТА ВАШЕГО КОМПЬЮТЕРА

Внимание!

В данной версии приложения отсутствует компонент **Контроль целостности приложений** для компьютеров под управлением Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista или Microsoft Windows Vista x64.

Антивирус Касперского защищает не только от известных угроз, но и от новых, информация о которых отсутствует в базах приложения. Это обеспечивает специально разработанный компонент – *Проактивная защита*.



Необходимость в проактивной защите назрела с тех пор, как скорость распространения вредоносных программ стала превышать скорость обновления антивирусной защиты, способной обезвредить эти угрозы. Реактивные

технологии, на которых построена антивирусная защита, требуют как минимум одного фактического заражения новой угрозой, времени на анализ вредоносного кода, на добавление его в базы приложения и на обновление этих баз на компьютерах пользователей. За это время новая угроза может нанести огромный ущерб.

Превентивные технологии, на которых построена Проактивная защита Антивируса Касперского, позволяют избежать потери времени и обезвредить новую угрозу еще до того, как она нанесет вред вашему компьютеру. За счет чего это достигается? В отличие от реактивных технологий, где анализ выполняется на основании записей баз приложения, превентивные технологии распознают новую угрозу на вашем компьютере по последовательности действий, выполняемой некоторой программой. В поставку приложения включен набор критериев, позволяющих определять, насколько активность той или иной программы опасна. Если в результате анализа активности последовательность действий какой-либо программы вызывает подозрение, Антивирус Касперского применяет действие, заданное правилом для активности подобного рода.

Опасная активность определяется по совокупности действий программы. Например, при обнаружении таких действий как самокопирование некоторой программы на сетевые ресурсы, в каталог автозапуска, системный реестр, а также последующая рассылка копий, можно с большой долей вероятности предположить, что это программа – червь. К опасным действиям также относятся:

- изменения файловой системы;
- встраивание модулей в другие процессы;
- скрывание процессов в системе;
- изменение определенных ключей системного реестра Microsoft Windows.

Все опасные операции отслеживаются и блокируются Проактивной защитой.

В процессе работы Проактивная защита использует набор правил, включенных в поставку приложения, а также сформированных пользователем при работе с приложением. *Правило* – это набор критериев, определяющих совокупность подозрительных действий и реакцию Антивируса Касперского на них.

Отдельные правила предусмотрены для активности приложений, контроля изменений системного реестра и запускаемых на компьютере программ. Вы можете изменять правила по своему усмотрению, добавляя, удаляя или изменяя их. Правила могут быть запрещающими или разрешающими.

Рассмотрим алгоритм работы Проактивной защиты:

1. Сразу после запуска компьютера Проактивная защита анализирует следующие аспекты:
 - *Действия каждого запускаемого на компьютере приложения.* История выполняемых действий и их последовательность фиксируется и сравнивается с последовательностью, характерной для опасной активности (база видов опасной активности включена в поставку Антивируса Касперского и обновляется вместе с базами приложения).
 - *Целостность программных модулей* установленных на вашем компьютере приложений, что позволяет избежать подмены модулей приложения, встраивания в них вредоносного кода.
 - *Каждую попытку изменения системного реестра* (удаление, добавление ключей системного реестра, ввод значений для ключей в недопустимом формате, препятствующем их просмотру и редактированию, и т.д.).
2. Анализ производится на основании разрешающих и запрещающих правил Проактивной защиты.
3. В результате анализа возможны следующие варианты поведения:
 - Если активность удовлетворяет условиям разрешающего правила Проактивной защиты либо не подпадает ни под одно запрещающее правило, она не блокируется.
 - Если активность описана в запрещающем правиле, дальнейшая последовательность действий компонента соответствует инструкциям, указанным в правиле. Обычно такая активность блокируется. На экран выводится уведомление, где указывается приложение, тип его активности, история выполненных действий. Вам нужно самостоятельно принять решение, запретить или разрешить такую активность. Вы можете создать правило для такой активности и отменить выполненные действия в системе.

Проактивная защита осуществляется в строгом соответствии с параметрами (см. рис. 35), определяющими:

- *Подвергается ли контролю активность приложений на вашем компьютере.*

Такой режим работы Проактивной защиты регулируется флажком  **Включить анализ активности.** По умолчанию режим включен, что обеспечивает строгий анализ действий любой программы, запускаемой на компьютере. Выделен набор опасной активности, для ка-

ждой из которых вы можете настроить порядок обработки приложений (см. п. 10.1 на стр. 123) с такой активностью. Также предусмотрена возможность формирования исключений Проактивной защиты, где вы можете отменить контроль активности избранных приложений.

- *Включен ли контроль целостности приложений.*

Данная функциональность отвечает за целостность модулей установленных на вашем компьютере приложений и регулируется флажком **Включить контроль целостности**. Целостность отслеживается по составу модулей программы и контрольной сумме образа самой программы. Вы можете сформировать правила контроля (см. п. 10.2 на стр. 127) за целостностью модулей какого-либо приложения, для этого необходимо внести это приложение в список контролируемых.

Данный компонент Проактивной защиты отсутствует в приложении, установленном под управлением операционных систем Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista или Microsoft Windows Vista x64.

- *Обеспечивается ли контроль изменений системного реестра.*

По умолчанию флажок **Включить мониторинг системного реестра** установлен, а значит, Антивирус Касперского анализирует все попытки внести изменения в контролируемые ключи системного реестра операционной системы.

Вы можете создать собственные правила (см. п. 10.3.2 на стр. 134) контроля в зависимости от ключа реестра Microsoft Windows.

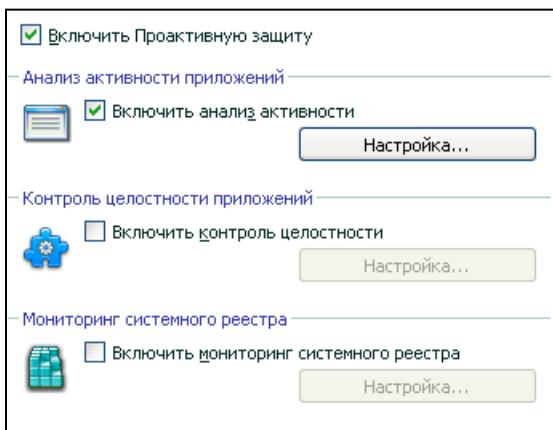


Рисунок 35. Параметры проактивной защиты

Вы можете настроить исключения (см. п. 6.9.1 на стр. 71) для модулей Проактивной защиты, а также сформировать список доверенных приложений (см. п. 6.9.2 на стр. 76).

В данном разделе Руководства будут детально рассмотрены все перечисленные выше аспекты.

10.1. Правила контроля активности

Обратите внимание, что настройка контроля активности в приложении, установленном под управлением операционных систем Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista или Microsoft Windows Vista x64, отличается от приложения, установленного под управлением других операционных систем.

Информация о настройке контроля активности для перечисленных операционных систем приведена в конце данного раздела.

Активность приложений на вашем компьютере контролируется Антивирусом Касперского. В состав приложения входит набор описаний событий, которые могут трактоваться как опасные. Для каждого такого события создано правило. Если активность какого-либо приложения классифицируется как опасное событие, Проактивная защита будет следовать инструкциям, указанным в правиле для такого события.

Установите флажок **Включить анализ активности**, чтобы начать контролировать активность приложений.

Рассмотрим некоторые виды событий, происходящих в системе, которые будут трактоваться приложением как подозрительные:

- *Опасная активность (анализ поведения).* Антивирус Касперского анализирует активность приложений, установленных на компьютере, и на основании списка правил, составленного специалистами «Лаборатории Касперского», обнаруживает опасные или подозрительные действия приложений. К таким действиям, например, относятся скрытая установка программ, самокопирование.
- *Запуск браузера с параметрами.* Анализ данного вида активности позволяет обнаруживать попытки скрытого запуска браузера с параметрами. Такая активность характерна для запуска веб-браузера из какого-либо приложения с определенными параметрами командной строки: например, при использовании ссылки на некоторый адрес в интернете из рекламного письма, пришедшего в ваш почтовый ящик.
- *Внедрение в процесс* – добавление в процесс некоторой программы исполняемого кода или создание дополнительного потока. Такая активность характерна для троянских программ.

- *Появление скрытого процесса (Rootkit)*. Rootkit – это набор программ, использующихся для сокрытия в системе вредоносных программ и их процессов. Антивирус Касперского проводит анализ операционной системы на предмет наличия скрытых процессов.
- *Внедрение оконных перехватчиков*. Такая активность используется при попытке считывания паролей и другой конфиденциальной информации, отображаемой в диалоговых окнах операционной системы. Антивирус Касперского отслеживает данную активность при попытке перехвата информации, которой обмениваются операционная система и диалоговое окно.
- *Подозрительные значения в реестре*. Системный реестр – это база данных для хранения системных и пользовательских параметров, определяющих работу операционной системы Microsoft Windows, а также любых служб, установленных на компьютере. Вредоносные программы, пытаясь скрыть свое присутствие в системе, прописывают в ключи реестра некорректные значения. Антивирус Касперского анализирует записи системного реестра на предмет наличия подозрительных значений.
- *Подозрительная активность в системе*. Программа анализирует действия, выполняемые операционной системой Microsoft Windows и выявляет подозрительную активность. Примером подозрительной активности является нарушение целостности, что подразумевает под собой изменение одного или нескольких модулей контролируемого приложения с момента предыдущего запуска.
- *Обнаружение клавиатурных перехватчиков*. Такая активность используется при перехвате вредоносными программами информации, вводимой с клавиатуры.
- *Защита Диспетчера задач Microsoft Windows*. Антивирус Касперского защищает Диспетчер задач от внедрения вредоносных модулей, деятельность которых направлена на блокирование работы Диспетчера.

Список опасной активности пополняется автоматически при обновлении Антивируса Касперского и отредактировать его нельзя. Вы можете:

- отказаться от контроля той или иной активности, сняв флажок , установленный рядом с ее названием;
- изменить правило, в соответствии с которым действует Проактивная защита при обнаружении опасной активности;
- составить список исключений (см. п. 6.9 на стр. 70), перечислив приложения, активность которых вы не считаете опасной.

Чтобы перейти к настройке контроля активности,

1. Откройте окно настройки приложения и выберите компонент **Проактивная защита** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Анализ активности приложений** (см. рис. 35).

Виды опасной активности, которые контролируются Проактивной защитой, приводятся в окне **Настройка: анализ активности** (см. рис. 36).

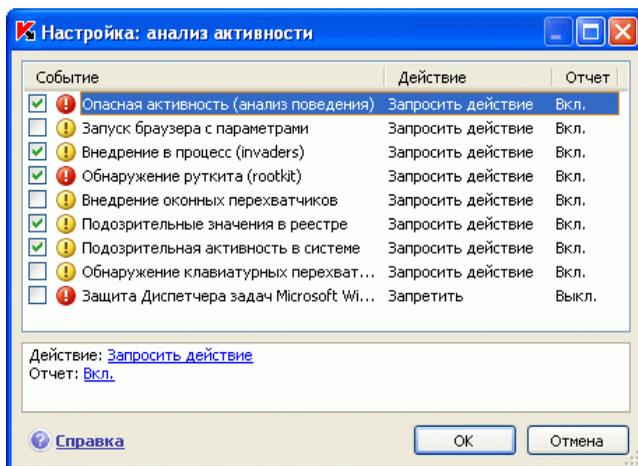


Рисунок 36. Настройка контроля активности приложений

Чтобы изменить правило контроля опасной активности, выберите его в списке и в нижней части закладки задайте параметры правила:

- Определите реакцию Проактивной защиты на опасную активность.

В качестве реакции может быть задано одно из следующих действий: разрешить, запросить действие и завершить процесс. Щелкните левой клавишей мыши по ссылке с действием, пока она не примет нужное вам значение. Дополнительно к завершению процесса вы можете приложение, вызвавшее опасную активность, на карантин. Для этого воспользуйтесь ссылкой Вкл. / Выкл напротив соответствующего параметра. Для обнаружения скрытых процессов в системе вы можете дополнительно задать временное значение, с периодичностью в которое будет запускаться проверка.

- Укажите необходимость формирования отчета о выполненной операции. Для этого воспользуйтесь ссылкой Вкл. / Выкл.

Чтобы отказаться от контроля той или иной опасной активности, снимите флажок , установленный рядом с ее названием в списке опасных активностей.

Особенности настройки контроля активности приложений в Антивирусе Касперского под Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista или Microsoft Windows Vista x64:

Если компьютер работает под управлением перечисленных выше операционных систем, то контролируется только один вид событий, происходящих в системе, – *опасная активность (анализ поведения)*.

Для того чтобы кроме пользовательских процессов Антивирус Касперского контролировал активность системных процессов, установите флажок **Контролировать системные учетные записи** (см. рис. 37). По умолчанию данная возможность отключена.

Учетные записи регулируют доступ в систему, определяют пользователя и его рабочую среду, что предотвращает повреждение операционной системы или данных других пользователей. Системные процессы – это процессы, которые были запущены системной учетной записью.

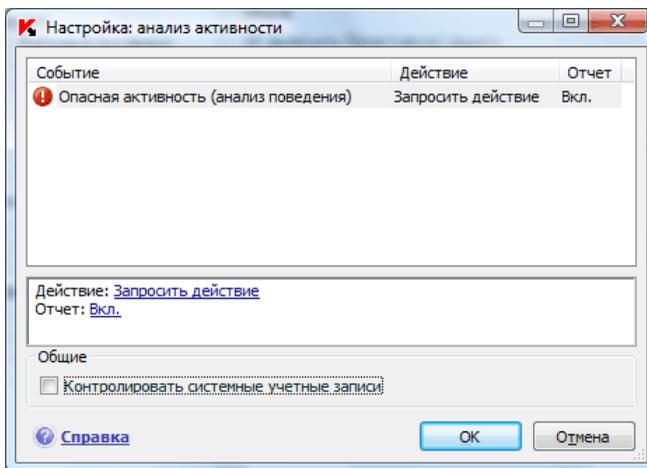


Рисунок 37. Настройка контроля активности приложений под Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64

10.2. Контроль целостности приложений

Данный компонент проактивной защиты не работает на компьютерах под управлением Microsoft Windows XP Professional x64 Edition, а также Microsoft Windows Vista и Microsoft Windows Vista x64.

Существует ряд критических для системы программ, которые могут быть использованы вредоносными программами для распространения, например, браузеры, почтовые клиенты и т.д. Как правило, это системные приложения, процессы, используемые для выхода в интернет и при работе с почтой и другими документами. Именно поэтому такие приложения являются *критическими* с точки зрения контроля их активности.

Проактивная защита контролирует критические приложения, анализирует их активность, целостность состава модулей данных приложений, запуск этими приложениями других процессов. В поставку Антивируса Касперского включен список критических приложений и для каждого из них создано свое правило, регламентирующее активность приложения. Вы можете пополнять этот список другими критическими, с вашей точки зрения, приложениями, а также удалять или редактировать правила для приложений поставляемого списка.

Кроме списка критических приложений существует набор доверенных модулей, разрешенных для загрузки во все контролируемые приложения. Например, таковыми являются модули, подписанные Microsoft Corporation. С высокой степенью вероятности активность приложений, в состав которых входят такие модули, не может быть вредоносной, поэтому строгий контроль над действиями не требуется. Специалисты «Лаборатории Касперского» сформировали список таких модулей для того чтобы снизить нагрузку на ваш компьютер при работе Проактивной защиты.

По умолчанию, компоненты, имеющие подпись Microsoft Corporation, автоматически попадают в список доверенных приложений. При необходимости мы можете добавлять или удалять компоненты из списка.

Контроль за процессами в системе регулируется флажком **Включить контроль целостности**. По умолчанию флажок не установлен. В случае контроля целостности каждое запускаемое приложение или модуль приложения проверяется на присутствие в списке критических или доверенных приложений. Если приложение присутствует в списке критических приложений, его активность подвергается контролю Проактивной защиты в соответствии с созданным для него правилом.

Чтобы перейти к настройке мониторинга процессов,

1. Откройте окно настройки приложения и выберите компонент **Проактивная защита** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Контроль целостности приложений** (см. рис. 35).

Рассмотрим подробнее работу с критическими и доверенными процессами.

10.2.1. Настройка правил контроля критических приложений

Критические приложения – это исполняемые файлы программ, контроль за активностью которых имеет очень важное значение, поскольку такие программы используются вредоносными объектами для самораспространения.

Список критических приложений, сформированный специалистами «Лаборатории Касперского» и включенный в поставку приложения, приведен на закладке **Контролируемые приложения** (см. рис. 38). Для каждого такого приложения сформировано правило регламентирующее активность данного приложения. Вы можете редактировать существующие правила и создавать собственные.

Проактивная защита анализирует следующие операции с критическими приложениями: запуск, изменение состава модулей приложения и запуск приложения как дочернего процесса. Для каждой из перечисленных операций вы можете выбрать реакцию Проактивной защиты (разрешать или не разрешать операцию), а также указать необходимость фиксирования активности в отчете по работе компонента. По умолчанию практически для всех критических приложений операции запуска, изменения и запуска дочерних процессов разрешены.

Чтобы добавить приложение в список критических приложений и создать для него правило,

1. Нажмите на кнопку **Добавить** на закладке **Контролируемые приложения**. Будет открыто контекстное меню, в котором из пункта **Обзор** вы можете перейти в стандартное окно выбора файлов, или из пункта **Приложения** перейти к списку приложений, работающих в данный момент, и выбрать нужное. Приложение будет добавлено первым в список. Для него по умолчанию будет создано разрешающее правило. При первом запуске этого приложения будет сформирован список модулей, используемых во время запуска, именно они будут разрешены.

2. Выберите правило в списке и в нижней части закладки задайте параметры правила:

- Определите реакцию Проактивной защиты на попытку запуска, изменения состава или запуска критического приложения как дочернего процесса.

В качестве реакции может быть использовано одно из следующих действий: разрешить, запросить действие и запретить.левой клавишей мыши щелкайте по ссылке с действием, пока она не примет нужное вам значение.

- Укажите необходимость формирования отчета о выполненной операции. Для этого воспользуйтесь ссылкой записывать в отчет / не записывать в отчет.

Чтобы отказаться от контроля активности какого-либо приложения, вам достаточно снять флажок , установленный рядом с его именем.

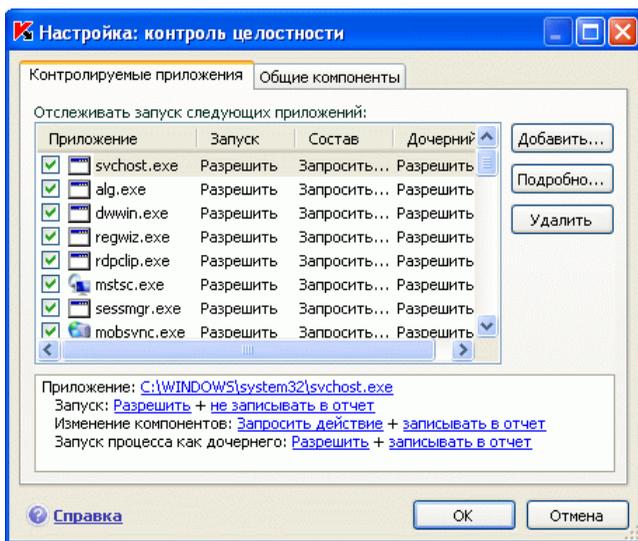


Рисунок 38. Настройка контроля целостности приложений

Для детального просмотра списка модулей выбранного приложения воспользуйтесь кнопкой **Подробнее**. В окне **Настройка: модули приложения** приведен список модулей, входящих в состав и используемых при запуске контролируемого приложения. Вы можете наполнять и редактировать список с помощью кнопок **Добавить** и **Удалить**, расположенных в правой части окна.

Также вы можете разрешать либо запрещать загрузку какого-либо модуля контролируемым приложением. По умолчанию для каждого модуля создается разрешающее правило. Для изменения действия выберите модуль в списке и воспользуйтесь кнопкой **Изменить**. В открывшемся окне установите необходимое действие.

Обратите внимание, что при первом запуске контролируемого приложения после установки Антивируса Касперского производится обучение до завершения работы приложения. В процессе обучения формируется список используемых приложением модулей. Правила контроля целостности будут применены при последующих запусках приложения.

10.2.2. Формирование списка общих компонентов

В Антивирусе Касперского предусмотрен список общих компонентов, разрешенных для загрузки во все контролируемые приложения. Этот список приведен на закладке **Общие компоненты** (см. рис. 39). Список включает модули, используемые Антивирусом Касперского, компоненты, подписанные Microsoft Corporation, а также добавленные пользователем компоненты.

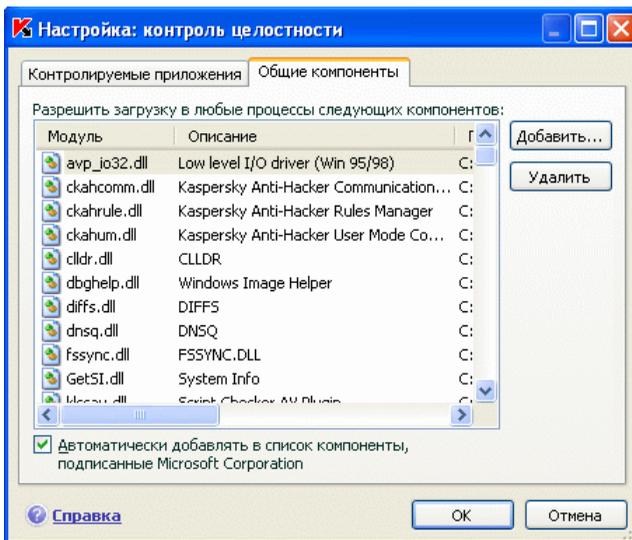


Рисунок 39. Настройка списка доверенных модулей

Вы можете устанавливать различные программы на ваш компьютер и для того чтобы модули, имеющие Microsoft Corporation, автоматически добав-

лялись в список доверенных модулей, установите флажок  **Автоматически добавлять в список компоненты, подписанные Microsoft Corporation**. В этом случае, если контролируемое приложение попытается загрузить модуль, имеющий подпись Microsoft Corporation, то загрузка данного модуля будет автоматически разрешена и модуль будет помещен в список общих компонентов.

Для пополнения списка доверенных модулей нажмите на кнопку **Добавить** и в стандартном окне выбора файлов выберите модуль.

10.3. Контроль изменений системного реестра

Одной из целей многих вредоносных программ является изменение реестра операционной системы на вашем компьютере. Это могут быть как безобидные программы-шутки, так и более опасные вредоносные программы, представляющие серьезную угрозу вашему компьютеру.

Так, например, вредоносные программы могут прописаться в ключ реестра, отвечающий за автоматический запуск приложений. В результате этого сразу после запуска операционной системы будут автоматически запущены вредоносные программы.

Специальный модуль Проактивной защиты отслеживает изменения объектов системного реестра. Работа данного модуля регулируется флажком  **Включить мониторинг системного реестра**.

Чтобы перейти к настройке контроля системного реестра,

1. Откройте окно настройки приложения и выберите компонент **Проактивная защита** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Мониторинг системного реестра** (см. рис. 35).

Список правил, регламентирующих работу с объектами реестра, уже сформирован специалистами «Лаборатории Касперского» и включен в поставку приложения. Операции с объектами реестра распределены по логическим группам, таким как *System Security*, *Internet Security* и т.д. Каждая такая группа включает объекты системного реестра и правила по работе с ними. Данный список обновляется вместе с обновлением приложения.

Полный список правил приведен в окне **Группы ключей реестра** (см. рис. 40).

Каждая группа правил имеет приоритет выполнения, который вы можете повышать или понижать с помощью кнопок **Вверх** и **Вниз**. Чем выше расположена группа в списке, тем выше приоритет ее выполнения. Если один и тот же объект реестра попадает в несколько групп, в первую очередь к та-

кому объекту будет применено правило из группы с более высоким приоритетом.

Отказаться от использования какой-либо группы правил можно следующими способами:

- Снять флажок рядом с именем группы. В этом случае группа правил останется в списке, но не будет использоваться.
- Удалить группу правил из списка. Не рекомендуется удалять группы, созданные специалистами «Лаборатории Касперского», поскольку они содержат список объектов системного реестра, наиболее часто используемые вредоносными программами.

Существует возможность создавать собственные группы контролируемых объектов системного реестра. Для этого в окне групп объектов нажмите на кнопку **Добавить**.

В открывшемся окне выполните следующие действия:

1. Введите имя новой группы объектов системного реестра в поле **Имя группы**.
2. Сформируйте список объектов системного реестра, которые будут входить в контролируемую группу, на закладке **Ключи** (см. п. 10.3.1 на стр. 133). Это может быть как один, так и несколько объектов.
3. Создайте правило для объектов реестра на закладке **Правила** (см. п. 10.3.2 на стр. 134). Вы можете создать несколько правил и определить приоритет их применения.

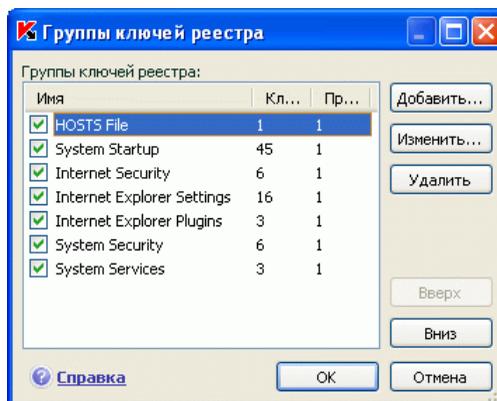


Рисунок 40. Контролируемые группы ключей системного реестра

10.3.1. Выбор объектов реестра для создания правила

Создаваемая группа объектов должна содержать хотя бы один объект системного реестра. Список объектов для правила формируется на закладке **Ключи**.

Чтобы добавить объект системного реестра,

1. Нажмите на кнопку **Добавить** в окне **Изменение группы** (см. рис. 41).
2. В открывшемся окне выберите объект или группу объектов системного реестра, для которой вы хотите создать правило контроля.
3. Укажите значение объекта или маску группы объектов, к которой вы хотите применить правило, в поле **Значение**.
4. Установите флажок **Включая вложенные ключи**, чтобы правило применялось ко всем вложенным ключам выбранного для объекта системного реестра.

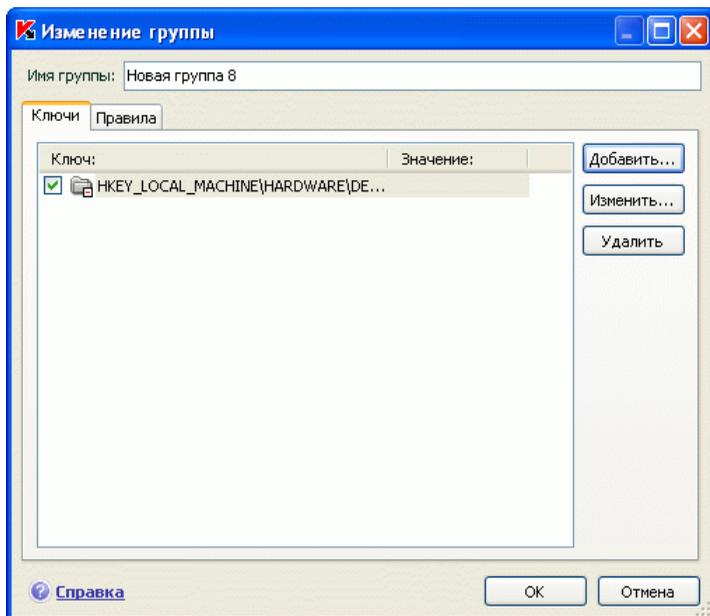


Рисунок 41. Добавление ключа реестра для контроля

Одновременное использование маски с символами * или ? и установленного флажка **Включая вложенные ключи** требуется только в случае, если данные символы используются в имени ключа.

Если с помощью маски выбрана группа объектов реестра и для нее указано конкретное значение, правило будет применено именно к указанному значению для любого ключа выбранной группы.

10.3.2. Создание правила для контроля ключей реестра

Правило контроля объектов системного реестра состоит из определения:

- приложения, к которому будет применено правило, если оно произведет попытку обращения к системному реестру;
- реакции приложения на попытку приложения выполнить ту или иную операцию с объектами системного реестра.

Итак, чтобы создать правило для выбранных объектов системного реестра,

1. Нажмите на кнопку **Создать** на закладке **Правила**. Обобщающее правило будет добавлено первым в список правил (см. рис. 42).
2. Выберите правило в списке и в нижней части закладки задайте параметры правила:
 - Укажите приложение.

По умолчанию правило создается для любого приложения. Чтобы правило распространялось на конкретное приложение, щелкните левой клавишей мыши по ссылке любое, она примет значение выбранное. Затем воспользуйтесь ссылкой укажите приложение. Будет открыто контекстное меню, в котором из пункта **Обзор** вы можете перейти в стандартное окно выбора файлов, или из пункта **Приложения** перейти к списку приложений, работающих в данный момент, и выбрать нужное.

- Определите реакцию Проактивной защиты на попытку выбранного приложения выполнить операцию чтения, изменения и удаления объектов системного реестра.

В качестве реакции может быть одно из следующих действий: разрешить, запросить действие и запретить. Щелкайте по ссылке с действием левой клавишей мыши, пока она не примет нужное вам значение.

ГЛАВА 11. ПОИСК ВИРУСОВ НА КОМПЬЮТЕРЕ

Одной из важных составляющих обеспечения антивирусной защиты компьютера является поиск вирусов в указанных пользователем областях. Антивирус Касперского 7.0 позволяет проверять на присутствие вирусов как отдельные объекты (файлы, папки, диски, сменные устройства), так и весь компьютер в целом. Проверка на вирусы позволяет исключить возможность распространения вредоносного кода, не обнаруженного компонентами постоянной защиты по тем или иным причинам.

В состав Антивируса Касперского 7.0 по умолчанию включены следующие задачи проверки:

Критические области

Проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты, исполняемые при старте системы, загрузочные сектора дисков, системные каталоги *Windows* и *system32*. Цель задачи – быстрое обнаружение в системе активных вирусов, без запуска полной проверки компьютера.

Мой Компьютер

Поиск вирусов на вашем компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов.

Объекты автозапуска

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

Поиск руткитов (rootkit)

Поиск на компьютере руткитов, обеспечивающих сокрытие вредоносных программ в операционной системе. Данные утилиты внедряются в систему, маскируя свое присутствие, а также наличие в системе процессов, каталогов, ключей реестра любых вредоносных программ, описанных в конфигурации руткита.

По умолчанию данные задачи выполняются с рекомендуемыми параметрами защиты. Вы можете изменять эти параметры (см. п. 11.4 на стр. 140), а также устанавливать расписание запуска задач (см. п. 6.6 на стр. 65).

Также предусмотрена возможность создавать собственные задачи (см. п. 11.3 на стр. 139) поиска вирусов и формировать расписание их запуска. Например, можно создать задачу проверки почтовых баз раз в неделю или задачу поиска вирусов в каталоге **Мои документы**.

Кроме того, вы можете проверить на вирусы любой объект (например, один из жестких дисков, на котором находятся программы и игры, почтовые базы, принесенные с работы, пришедший по почте архив и т.п.), не создавая для этого специальной задачи проверки. Выбрать объект для проверки можно из интерфейса Антивируса Касперского 7.0 или стандартными средствами операционной системы Microsoft Windows (например, в окне программы **Проводник** или на **Рабочем столе** и т.д.).

Полный список задач поиска вирусов, сформированных для вашего компьютера, можно просмотреть в разделе **Поиск вирусов** в левой части главного окна приложения.

Вы можете создать диск аварийного восстановления (см. п. 15.4 на стр. 185), который предназначен для восстановления системы после вирусной атаки, в результате которой повреждены системные файлы операционной системы и невозможна ее первоначальная загрузка. Для этого воспользуйтесь ссылкой [Создать диск аварийного восстановления](#).

11.1. Управление задачами поиска вирусов

Запуск задач проверки на вирусы осуществляется вручную или автоматически по сформированному расписанию (см. п. 6.7 на стр. 67).

Чтобы запустить задачу поиска вирусов вручную,

выберите имя задачи в разделе **Поиск вирусов** главного окна приложения и воспользуйтесь ссылкой [Запустить проверку](#).

Задачи, выполняющиеся в текущий момент, отображаются в контекстном меню, открываемом при нажатии правой кнопкой мыши по значку приложения в системной панели.

Чтобы приостановить задачу поиска вирусов,

выберите имя задачи в разделе **Поиск вирусов** главного окна приложения и воспользуйтесь ссылкой [Пауза](#). Проверка будет приостановлена до того момента, пока задача не будет запущена снова вручную или по расписанию. Для запуска проверки вручную нажмите на ссылку [Возобновить](#).

Чтобы остановить выполнение задачи,

выберите имя задачи в разделе **Поиск вирусов** главного окна приложения и воспользуйтесь ссылкой [Стоп](#). Проверка будет остановлена до того момента, пока задача не будет запущена снова вручную или по расписанию. При следующем запуске задачи вам будет предложено продолжить прерванную проверку или начать ее заново.

11.2. Формирование списка объектов проверки

Чтобы посмотреть список объектов, которые подлежат проверке при выполнении задачи, в разделе **Поиск вирусов** главного окна приложения выберите имя задачи (например, **Мой компьютер**). Список объектов будет представлен в правой части окна (см. рис. 43).

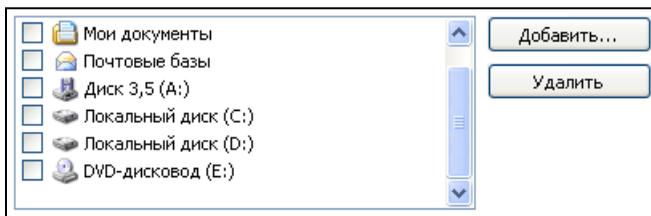


Рисунок 43. Список объектов для проверки

Для задач, созданных по умолчанию при установке приложения, списки объектов для проверки уже сформированы. При создании собственной задачи или при выборе объекта в рамках задачи проверки на вирусы отдельного объекта вы сами формируете список объектов.

Наполнение и редактирование списка объектов проверки осуществляется с помощью кнопок, расположенных справа от списка. Для добавления нового объекта проверки в список нажмите на кнопку **Добавить** и в открывшемся окне укажите объект для проверки.

Для удобства пользователей доступно добавление в область проверки таких категорий как почтовые базы, 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 и воспользуйтесь командой **Включая вложенные папки**.

Для удаления объекта выберите его в списке (при этом название объекта будет выделено серым фоном) и нажмите на кнопку **Удалить**. Вы можете временно отключать проверку отдельных объектов при выполнении какой-либо задачи, не удаляя их из списка. Для этого достаточно снять флажок напротив того объекта, который не требуется проверять.

Для запуска задачи проверки воспользуйтесь ссылкой [Запустить проверку](#).

Кроме того, вы можете выбрать объект для проверки стандартными средствами операционной системы Microsoft Windows, например, в окне програм-

мы **Проводник** или на **Рабочем столе** и т.д. (см. рис. 44). Для этого установите курсор мыши на имени выбранного объекта, правой клавишей мыши откройте контекстное меню Microsoft Windows и выберите пункт **Проверить на вирусы**.

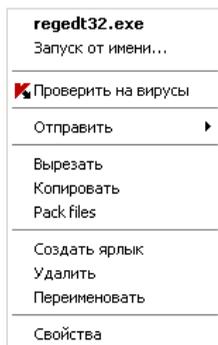


Рисунок 44. Проверка объекта из контекстного меню Microsoft Windows

11.3. Создание задач поиска вирусов

Для проверки объектов вашего компьютера на вирусы вы можете использовать встроенные задачи проверки, включенные в поставку приложения, а также создавать собственные задачи. Создание новой задачи происходит на основе уже имеющихся задач проверки.

Чтобы создать новую задачу проверки,

1. В разделе **Поиск вирусов** главного окна приложения выберите задачу, параметры которой наиболее приближены к вашим требованиям.
2. Откройте контекстное меню и выберите пункт **Сохранить как** либо воспользуйтесь ссылкой [Новая задача проверки](#).
3. В открывшемся окне введите имя новой задачи и нажмите на кнопку **ОК**. В результате задача с указанным именем появится в списке задач раздела **Поиск вирусов** главного окна приложения.

Внимание!

В приложении действует ограничение на количество задач, которые может создать пользователь. Максимальное количество – четыре задачи.

Новая задача наследует все параметры задачи, на основе которой она была создана. Поэтому вам потребуется провести дополнительную настройку: сформировать список объектов проверки (см. п. 11.2 на стр. 138), указать параметры, с которыми будет выполняться задача (см. п. 11.4 на стр. 140), а также, если требуется, настроить расписание (см. п. 6.6 на стр. 65) автоматического запуска.

Чтобы переименовать созданную задачу,

выберите задачу в разделе **Поиск вирусов** главного окна приложения и воспользуйтесь ссылкой [Переименовать](#).

В открывшемся окне введите новое имя для задачи и нажмите на кнопку **ОК**. В результате имя задачи в разделе **Поиск вирусов** будет изменено.

Чтобы удалить созданную задачу,

выберите задачу в разделе **Поиск вирусов** главного окна приложения и воспользуйтесь ссылкой [Удалить](#).

Подтвердите удаление задачи в окне запроса подтверждения. В результате задача будет удалена из списка задач раздела **Поиск вирусов**.

Внимание!

Операции переименования и удаления доступны только для задач, которые созданы вами.

11.4. Настройка задач поиска вирусов

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

Для того чтобы перейти к настройке параметров задачи,

откройте окно настройки приложения, выберите имя задачи в разделе **Поиск вирусов** и воспользуйтесь ссылкой [Настройка](#).

В окне настройки для каждой из задач вы можете:

- выбрать уровень безопасности, на основе параметров которого будет выполняться задача (см. п. 11.4.1 на стр. 141);
- перейти к подробной настройке уровня:
 - указать параметры, определяющие типы файлов, подверженные анализу на вирусы (см. п. 11.4.2 на стр. 142);

- настроить запуск задач от имени другой учетной записи (см. п. 6.6 на стр. 65);
- указать дополнительные параметры проверки (см. п. 11.4.3 на стр. 146);
- включить поиск руткитов (см. п. 11.4.4 на стр. 147) и использование методов эвристического анализа (см. п. 11.4.5 на стр. 148);
- восстановить параметры проверки, используемые по умолчанию (см. п. 11.4.6 на стр. 149);
- выбрать действие, которое будет применено при обнаружении зараженного/ возможно зараженного объекта (см. п. 11.4.7 на стр. 149);
- сформировать расписание автоматического запуска задачи (см. п. 6.7 на стр. 67).

Кроме того, вы можете установить единые параметры запуска для всех задач (см. п. 11.4.8 на стр. 152).

В данном разделе Руководства будут детально рассмотрены все перечисленные выше параметры настройки задачи.

11.4.1. Выбор уровня безопасности

Каждая задача проверки на вирусы обеспечивает проверку объектов на одном из следующих уровней (см. рис. 45):

Максимальная защита – максимально полная проверка всего компьютера или отдельного его диска, каталога, файла. Данный уровень мы рекомендуем использовать в случае подозрения вашего компьютера на заражение вирусом.

Рекомендуемый. Параметры данного уровня рекомендованы экспертами «Лаборатории Касперского». Они определяют проверку тех же объектов, что на уровне **Максимальная защита**, за исключением файлов почтовых форматов.

Максимальная скорость – уровень с параметрами, которые позволяют вам комфортно работать с приложениями, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых файлов на данном уровне сокращен.

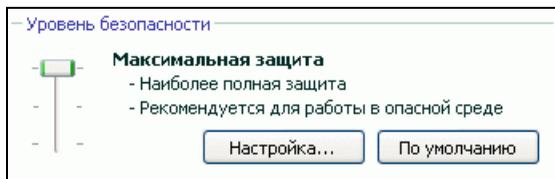


Рисунок 45. Выбор уровня безопасности при проверке объектов на вирусы

По умолчанию проверка объектов осуществляется на **Рекомендуемом** уровне.

Вы можете повысить или понизить степень проверки объектов, выбрав соответствующий уровень или изменив параметры текущего уровня.

Для того чтобы изменить уровень безопасности,

переместите ползунок по шкале. Регулируя уровень безопасности, вы определяете соотношение между скоростью выполнения проверки и количеством проверяемых файлов: чем меньше файлов подвергается анализу на присутствие вирусов, тем выше скорость проверки.

Если ни один из перечисленных уровней безопасности файлов не соответствует вашим требованиям, вы можете выполнить дополнительную настройку параметров проверки. Для этого рекомендуется выбрать наиболее близкий к вашим требованиям уровень в качестве базового и отредактировать его параметры. В этом случае название уровня безопасности будет изменено на **Другой**.

Чтобы изменить параметры текущего уровня безопасности,

1. Откройте окно настройки приложения и выберите имя задачи проверки в разделе **Поиск вирусов**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 45).
3. В открывшемся окне отредактируйте параметры защиты файлов и нажмите на кнопку **ОК**.

11.4.2. Определение типов проверяемых объектов

Указывая тип проверяемых объектов, вы определяете, файлы какого формата, размера и на каких дисках будут проверяться при выполнении данной задачи.

Тип файлов для проверки на вирусы определяется в разделе **Типы файлов** (см. рис. 46). Выберите один из трех вариантов:

- Проверять все файлы.** В данном случае проверке будут подвергаться все без исключения файлы.
- Проверять программы и документы (по содержимому).** При выборе такой группы приложение будет проверять только потенциально заражаемые объекты – файлы, в которые может внедриться вирус.

Информация.

Существует ряд файловых форматов, вероятность внедрения в которые вредоносного кода и его последующая активация достаточно низка. Примером такого файла является файл *txt*-формата.

И наоборот, есть файловые форматы, которые содержат или могут содержать исполняемый код. Примером таких объектов являются файлы форматов *exe*, *dll*, *doc*. Риск внедрения и активации в такие файлы вредоносного кода достаточно высок.

Прежде чем приступать к поиску вирусов в объекте, выполняется анализ его внутреннего заголовка на предмет формата файла (*txt*, *doc*, *exe* и т.д.).

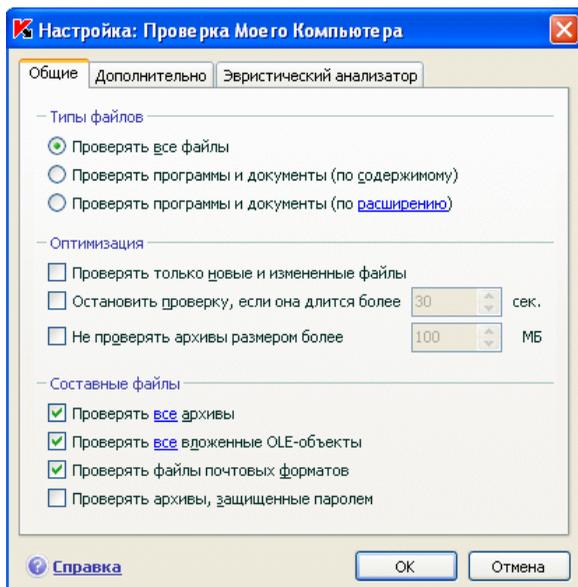


Рисунок 46. Настройка параметров проверки

- Проверять программы и документы (по расширению).** В этом случае приложение будет проверять только потенциально заражаемые файлы, при этом формат файла будет определяться на основании его расширения. Воспользовавшись ссылкой [расширению](#), вы можете ознакомиться со списком расширений файлов, которые подвергаются проверке в данном случае (см. п. А.1 на стр. 232).

Совет.

Не стоит забывать, что злоумышленник может отправить вирус на ваш компьютер в файле с расширением txt, хотя на самом деле он может быть исполняемым файлом, переименованным в txt-файл. Если вы выберете вариант **Проверять программы и документы (по расширению)**, то такой файл будет пропущен в процессе проверки. Если же выбран вариант **Проверять программы и документы (по содержимому)**, невзирая на расширение, приложение проанализирует заголовок файла, в результате чего выяснится, что файл имеет exe-формат. Такой файл будет подвергнут тщательной проверке на вирусы.

В разделе **Оптимизация** можно сделать оговорку, что проверять на вирусы следует только новые файлы и те, что изменились с момента предыдущего их анализа. Такой режим работы позволяет заметно сократить время проверки и увеличить скорость работы приложения. Для этого необходимо установить флажок **Проверять только новые и измененные файлы.** Этот режим работы распространяется как на простые, так и на составные файлы.

Также в разделе **Оптимизация** вы можете установить ограничение на время проверки и максимальный размер одного объекта:

- Остановить проверку, если она длится более...сек.** Установите флажок для ограничения проверки одного объекта по времени и в поле справа укажите максимально допустимое время проверки объекта. В результате, если данное временное значение будет превышено, объект будет исключен из проверки.
- Не проверять архивы размером более...МБ.** Установите флажок для ограничения проверки одного объекта по размеру и в поле справа укажите максимально допустимый размер объекта. В результате, если данное значение будет превышено, объект будет исключен из проверки.

В разделе **Составные файлы** укажите, какие составные файлы необходимо анализировать на присутствие вирусов:

- Проверять все/только новые архивы** – проверять архивы форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

Внимание!

Удаление архивов, в которых Антивирус Касперского не поддерживает лечение (например, HA, UUE, TAR), не происходит в автоматическом режиме, даже если выбрано действие автоматически лечить либо удалять, если лечение невозможно.

Для удаления подобных архивов воспользуйтесь ссылкой [Удалить архив](#) в окне уведомления об обнаружении опасного объекта. Данное уведомление выводится на экран после запуска обработки обнаруженных в ходе проверки объектов. Также зараженный архив можно удалить с компьютера вручную.

- Проверять все /только новые вложенные OLE-объекты** – проверять погруженные в файл объекты (например, Excel-таблица или макрос, внедренный в файл Microsoft Word, вложение почтового сообщения и т.д.).

Для каждого типа составного файла вы можете выбрать, 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 в разделе **Оптимизация** установлен режим проверки только новых и измененных файлов, выбор типа проверяемых составных файлов будет недоступен.

- Проверять файлы почтовых форматов** – проверять файлы почтовых форматов, а также почтовые базы данных. При включенном флажке Антивирус Касперского разбирает файл почтового формата и анализирует на наличие вирусов каждый компонент почтового сообщения (тело письма, вложение). Если флажок снят, файл почтового формата проверяется как единый объект.

Обратите внимание на следующие особенности проверки почтовых баз, защищенных паролем:

- Антивирус Касперского обнаруживает вредоносный код в базах Microsoft Office Outlook 2000, но не лечит их;
- приложение не поддерживает поиск вредоносного кода в защищенных почтовых базах Microsoft Office Outlook 2003.

- Проверять архивы, защищенные паролем** – включить проверку архивов, защищенных паролем. В данном случае перед проверкой объектов, содержащихся в архиве, на экран будет выведен запрос пароля. Если флажок не установлен, защищенные архивы будут пропущены при проверке.

11.4.3. Дополнительные параметры поиска вирусов

Кроме настройки основных параметров проверки на вирусы вы можете установить дополнительные параметры (см. рис. 47):

- ✔ **Включить технологию iChecker** – использовать технологию, позволяющую увеличить скорость проверки за счет исключения некоторых объектов. Исключение объекта из проверки осуществляется по специальному алгоритму, учитывающему дату выпуска баз приложения, дату предыдущей проверки объекта, а также изменение параметров проверки.

Например, у вас есть файл архива, который был проверен приложением 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 базы приложения, архив будет проверен повторно.

Технология iChecker™ имеет ограничение: она не работает с файлами больших размеров, а также применима только к объектам с известной приложению Kaspersky Internet Security структурой (например, файлы *exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar*).

- ✔ **Включить технологию iSwift**. Данная 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 также применима только к объектам, расположенным в файловой системе NTFS.
- ✔ **Показывать обнаруженные опасные объекты на закладке отчета «Обнаружено»** – отображать список обнаруженных при проверке угроз на закладке **Обнаружено** окна отчета (см. п. 15.3.2 на стр. 181). Отключение данной функции может быть полезно при специальной проверке, например, тестовых коллекций для увеличения скорости проверки.
- ✔ **Уступать ресурсы другим приложениям** – приостанавливать выполнение данной задачи проверки на вирусы, если ресурсы процессора заняты другими приложениями.

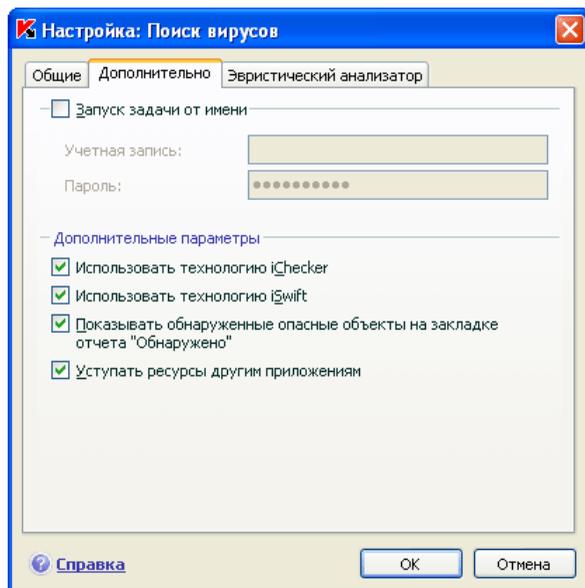


Рисунок 47. Дополнительная настройка проверки

11.4.4. 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, каталогов, ключей реестра любых вредоносных программ, описанных в конфигурации руткита.

Поиск руткитов может выполняться любой задачей поиска вирусов (при условии, что данная возможность включена в настройках конкретной задачи), однако специалисты «Лаборатории Касперского» сформировали и оптимально настроили отдельную задачу поиска вредоносных программ данного типа.

Для включения поиска руткитов установите флажок **Включить обнаружение руткитов (rootkit)** в блоке **Поиск руткитов (rootkit)**. Если поиск включен, вы можете установить детальный уровень обнаружения руткитов, выбрав флажок **Включить расширенный поиск руткитов**. В данном случае будет выполняться тщательный поиск данных программ путем анализа большего количества объектов разного типа. По умолчанию флажки сняты, поскольку включение данного режима требует значительных ресурсов операционной системы.

Для настройки поиска руткитов:

1. Откройте окно настройки приложения и выберите имя задачи в разделе **Поиск вирусов**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** (см. рис. 45) и в открывшемся окне перейдите на закладку **Эвристический анализатор** (см. рис. 48).

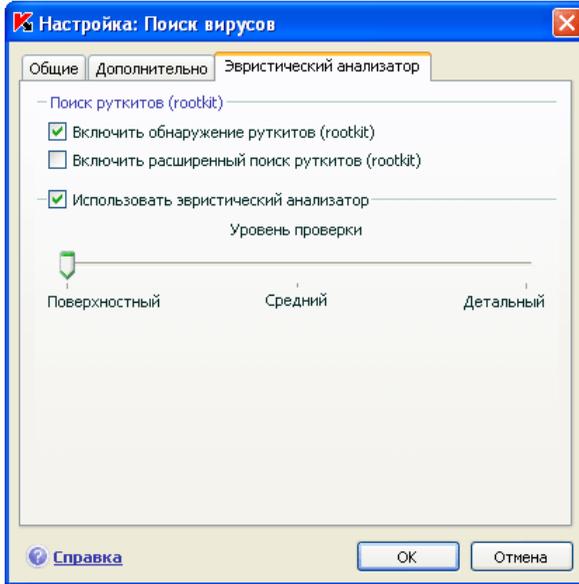


Рисунок 48. Настройка параметров поиска руткитов и использования методов эвристики

11.4.5. Использование методов эвристического анализа

Методы эвристического анализа используются в работе некоторых компонентов постоянной защиты, а также задач поиска вирусов (подробнее см. п. 7.2.4 на стр. 90).

На закладке **Эвристический анализатор** (см. рис. 48) вы можете включать/отключать использование эвристических методов обнаружения новых угроз в рамках работы задач поиска вирусов. Для этого выполните следующие действия:

1. Откройте окно настройки приложения и выберите имя задачи в разделе **Поиск вирусов**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень безопасности** и в открывшемся окне перейдите на закладку **Эвристический анализатор**.

Для использования методов эвристики установите флажок **Использовать эвристический анализатор**. Дополнительно вы можете выбрать уровень детализации проверки, для этого передвиньте бегунок в одну из позиций: **поверхностный**, **средний** или **детальный**.

11.4.6. 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,

1. Откройте окно настройки приложения и выберите имя задачи в разделе **Поиск вирусов**.
2. Нажмите на кнопку **По умолчанию** в блоке **Уровень безопасности** (см. рис. 45).

11.4.7. Выбор действия над объектами

Если в результате проверки объекта на вирусы выясняется, что он заражен или подозревается на заражение, дальнейшие операции приложения 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.

Чтобы изменить действие над объектом,

откройте окно настройки приложения и выберите имя задачи в разделе **Поиск вирусов**. Все возможные действия приведены в соответствующем блоке (см. рис. 49).

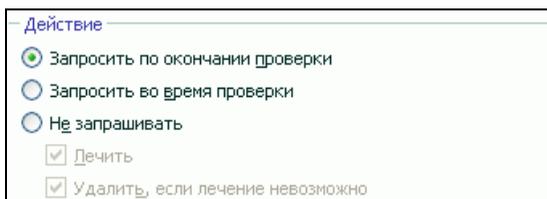


Рисунок 49. Выбор действия над опасным объектом

Если в качестве действия вы выбрали	При обнаружении зараженного/ возможно зараженного объекта
<input checked="" type="radio"/> Запросить по окончании проверки	Приложение откладывает обработку объектов до конца проверки. По окончании проверки на экран будет выведено окно статистики со списком обнаруженных объектов, и вам будет предложено провести обработку объектов.
<input checked="" type="radio"/> Запросить во время проверки	Приложение выводит на экран предупреждающее сообщение, содержащее информацию о том, каким вредоносным кодом заражен / возможно заражен объект, и предлагает на выбор одно из дальнейших действий.

Если в качестве действия вы выбрали	При обнаружении зараженного/ возможно зараженного объекта
<input type="radio"/> Не запрашивать	<p>Приложение фиксирует информацию об обнаруженных объектах в отчете, не обрабатывая их и не уведомляя пользователя. Не рекомендуется устанавливать данный режим работы приложения, поскольку зараженные и возможно зараженные объекты остаются на вашем компьютере и избежать заражения практически невозможно.</p>
<input type="radio"/> Не запрашивать <input checked="" type="checkbox"/> Лечить	<p>Приложение, не запрашивая подтверждения пользователя, выполняет попытку лечения обнаруженного объекта. Если попытка лечения не удалась, объекту присваивается статус <i>возможно зараженный</i>, и он помещается на карантин (см. п. 15.1 на стр. 171). Информация об этом фиксируется в отчете (см. п. 15.3 на стр. 177). Позже можно попытаться вылечить этот объект.</p>
<input type="radio"/> Не запрашивать <input checked="" type="checkbox"/> Лечить <input checked="" type="checkbox"/> Удалить, если лечение невозможно	<p>Приложение, не запрашивая подтверждения пользователя, выполняет попытку лечения обнаруженного объекта. Если попытка лечения объекта не удалась, он удаляется.</p>
<input type="radio"/> Не запрашивать <input checked="" type="checkbox"/> Лечить <input checked="" type="checkbox"/> Удалить	<p>Приложение автоматически удаляет объект.</p>

Перед лечением или удалением объекта Антивирус Касперского формирует его резервную копию и помещает ее в резервное хранилище (см. п. 15.2 на стр. 175) на тот случай, если понадобится восстановить объект или появится возможность его вылечить.

11.4.8. Назначение единых параметров проверки для всех задач

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

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

Для того чтобы назначить единые параметры проверки для всех задач:

1. Откройте окно настройки приложения и выберите раздел **Поиск вирусов**.
2. Установите параметры проверки: выберите уровень безопасности (см. п. 11.4.1 на стр. 141), произведите дополнительную настройку уровня, укажите действие над объектами (см. п. 11.4.7 на стр. 149).
3. Для применения установленных параметров ко всем задачам нажмите на кнопку **Применить** в блоке **Параметры других задач**. Подтвердите назначение единых параметров в окне запроса подтверждения.

ГЛАВА 12. ТЕСТИРОВАНИЕ РАБОТЫ АНТИВИРУСА КАСПЕРСКОГО

После установки и настройки Антивируса Касперского мы рекомендуем вам проверить правильность параметров и корректность работы приложения с помощью тестового «вируса» и его модификаций.

12.1. Тестовый «вирус» EICAR и его модификации

Тестовый «вирус» был специально разработан организацией  (The European Institute for Computer Antivirus Research) для проверки работы антивирусных продуктов.

Тестовый «вирус» НЕ ЯВЛЯЕТСЯ ВИРУСОМ и не содержит программного кода, который может навредить вашему компьютеру, 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.

Файл, который вы загрузили с сайта компании EICAR, содержит тело стандартного тестового «вируса». Антивирус Касперского обнаруживает его, присваивает тип **вирус** и выполняет действие, установленное для объекта с таким типом.

Для того чтобы проверить реакцию Антивируса Касперского при обнаружении объектов других типов, вы можете модифицировать содержание стандартного тестового «вируса», добавив к нему один из префиксов (см. таблицу).

Префикс	Статус для тестового «вируса»	Аналог действия при обработке объекта приложением
Префикс отсутствует, стандартный тестовый «вирус»	Файл содержит тестовый «вирус». Лечение невозможно.	Приложение идентифицирует данный объект как вредоносный, не подвергающийся лечению и выполняет удаление объекта.
CORR-	Поврежден.	Приложение получило доступ к объекту, но не может проверить его, поскольку объект поврежден (например, нарушена структура объекта, неверный формат файла).
SUSP- WARN-	Файл содержит тестовый «вирус» (модификация). Лечение невозможно.	Данный объект является модификацией известного вируса либо неизвестным вирусом. На момент обнаружения базы приложения не содержат описания процедуры лечения данного объекта. Приложение перемещает объект на карантин для последующей обработки с обновленными базами.
ERRO-	Ошибка обработки.	В ходе обработки объекта возникла ошибка: приложение не может получить доступ к объекту проверки, поскольку нарушена целостность объекта (например, нет конца многотомного архива) либо отсутствует связь с ним (если проверяется объект на сетевом ресурсе).
CURE-	Файл содержит тестовый «вирус». Лечение возможно. Объект подвергается лечению, при этом текст тела "вируса" изменяется на CURE.	Объект содержит вирус, поддающийся лечению. Приложение выполняет антивирусную обработку объекта, после которой он будет полностью вылечен.

Префикс	Статус для тестового «вируса»	Аналог действия при обработке объекта приложением
DELE-	Файл содержит тестовый «вирус». Лечение невозможно.	Данный объект содержит неизлечимый вирус либо является троянской программой. Приложение удаляет данные объекты.

В первом столбце таблицы приведены префиксы, которые нужно добавить в начало строки стандартного тестового «вируса». Во втором столбце описаны статусы и реакция Антивируса Касперского на различные типы тестового «вируса». Третий столбец содержит информацию об обработке приложением объектов с аналогичными статусами.

Действия над каждым из объектов определяются значениями параметров антивирусной проверки.

12.2. Проверка Файлового Антивируса

Для проверки работоспособности Файлового Антивируса;

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации (см. п. 12.1 на стр. 153), а также созданные вами модификации тестового «вируса».
2. Разрешите запись в отчет всех событий, для того чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя. Для этого установите флажок **Записывать некритические события** в разделе **Отчеты и файлы данных** окна настройки приложения (см. п. 15.3.1 на стр. 180).
3. Запустите файл тестового «вируса» или его модификацию на выполнение.

Файловый Антивирус перехватит обращение к файлу, проверит его и уведомит вас об обнаружении опасного объекта:



Рисунок 50. Обнаружен опасный объект

Выбирая различные варианты действий над обнаруженным объектом, вы сможете проверить реакцию Файлового Антивируса при обнаружении объектов различных типов.

Полный результат работы Файлового Антивируса можно посмотреть в отчете по работе компонента.

12.3. Проверка задачи Поиска вирусов

Для проверки задачи Поиска вирусов,

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации (см. п. 12.1 на стр. 153), а также созданные вами модификации тестового «вируса».
2. Создайте новую задачу поиска вирусов (см. п. 11.3 на стр. 139) и в качестве объекта проверки выберите папку, содержащую набор тестовых «вирусов» (см. п. 11.2 на стр. 138).
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. Для этого установите флажок **Записывать некритические события** в разделе **Отчеты и файлы данных** окна настройки приложения (см. п. 15.3.1 на стр. 180).

4. Запустите задачу (см. п. 11.1 на стр. 137) поиска вирусов на выполнение.

При проверке, по мере обнаружения подозрительных или зараженных объектов, на экран будут выведены уведомления с информацией об объекте и запросом дальнейшего действия у пользователя:

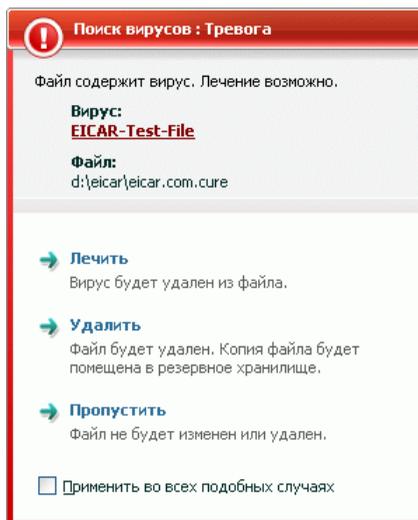


Рисунок 51. Обнаружен опасный объект

Таким образом, выбирая различные варианты действий, вы сможете проверить реакцию Антивируса Касперского при обнаружении объектов различных типов.

Полный результат выполнения задачи поиска вирусов можно посмотреть в отчете по работе компонента.

ГЛАВА 13. ОБНОВЛЕНИЕ ПРИЛОЖЕНИЯ

Поддержка защиты в актуальном состоянии – залог безопасности вашего компьютера. 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 приложения подразумевает загрузку и установку на ваш компьютер:

- **Баз Антивируса и сетевых драйверов**

Защита информации на вашем компьютере обеспечивается на основании баз приложения. Компоненты защиты используют их при поиске опасных объектов на вашем компьютере и их обезвреживании. Базы ежечасно пополняются записями о новых угрозах и способах борьбы с ними. Поэтому настоятельно рекомендуется регулярно обновлять их.

Кроме того, наряду с базами Антивируса обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

В предыдущих версиях антивирусных приложений «Лаборатории Касперского» поддерживалась работа с разными наборами баз: *стандартным* или *расширенным набором*. Их отличие состояло в типах опасных объектов, от которых они защищали ваш компьютер. В Антивирусе Касперского вам не нужно заботиться о выборе подходящего набора баз. Теперь при работе наших продуктов используются базы, которые позволяют защищать от различных видов вредоносных и потенциально-опасных объектов.

- **Модулей приложения**

Помимо баз приложения вы можете обновлять и внутренние модули Антивируса Касперского. Пакеты обновлений периодически выпускаются «Лабораторией Касперского».

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.

Для успешной загрузки обновлений с серверов необходимо, чтобы ваш компьютер был подключен к интернету. Если выход в интернет осуществляется через прокси-сервер, то вам необходимо настроить параметры подключения (см. п. 15.7 на стр. 193) к нему.

В случае если у вас нет доступа к серверам обновлений «Лаборатории Касперского» (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.

Загрузка обновлений выполняется в одном из следующих режимов:

- *Автоматически.* Антивирус Касперского с заданной периодичностью проверяет наличие пакета обновлений в источнике обновлений. Частота проверки может увеличиваться во время вирусных эпидемий и сокращаться вне их. При обнаружении свежих обновлений приложение скачивает их и устанавливает на компьютер. Такой режим используется по умолчанию.
- *По расписанию.* Обновление приложения производится в соответствии с установленным графиком.
- *Вручную.* В этом случае вы самостоятельно запускаете обновление приложения.

В процессе обновления модули приложения и базы на вашем компьютере сравниваются с расположенными в источнике обновлений. В случае если на вашем компьютере установлена последняя версия баз и модулей, на экран выдается информационное сообщение об актуальности защиты вашего компьютера. Если базы и модули отличаются, то на ваш компьютер 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 (см. п. 13.2 на стр. 160) необходима, например, в том случае, если вы обновили базы и в процессе работы они повредились. Вы сможете вернуться к предыдущему варианту баз, а позже попробовать обновить их еще раз.

Одновременно с обновлением приложения вы можете выполнять копирование полученных обновлений в локальный источник (см. п. 13.3.3 на стр. 165). Данный сервис позволяет обновлять базы приложения и модули, используемые приложениями версии 7.0, на компьютерах сети в целях экономии интернет-трафика.

13.1. Запуск обновления

В любой момент вы можете запустить обновление приложения. Оно будет производиться из выбранного вами источника обновлений (см. п. 13.3.1 на стр. 161).

Запустить обновление приложения вы можете:

- из контекстного меню (см. п. 4.2 на стр. 45);
- из главного окна приложения (см. п. 4.3 на стр. 47).

Чтобы запустить обновление приложения из контекстного меню,

1. Откройте меню по правой клавише мыши на значке приложения в системной панели.
2. Выберите пункт **Обновление**.

Чтобы запустить обновление из главного окна приложения,

1. Откройте главное окно приложения и выберите компонент **Обновление**.
2. Нажмите на ссылку Обновить базы.

Информация о процессе обновления будет отображаться в главном окне. Для получения подробной информации о процессе обновления воспользуйтесь ссылкой Подробнее. В результате будет открыт детальный отчет задачи обновления. Вы можете скрыть окно отчета. Для этого нажмите на кнопку **Закреть**. При этом обновление будет продолжено.

Обратите внимание, что при выполнении обновления одновременно будет произведено копирование обновлений в локальный источник, при условии, что данный сервис включен (см. п. 13.3.3 на стр. 165).

13.2. Откат последнего обновления

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

Возможность отката полезна, например, в том случае, если вы обновили базы, но в процессе обновления часть баз была повреждена в результате сбоя в соединении. Вы сможете вернуться к предыдущей версии баз, а позже попробовать обновить их еще раз.

Чтобы вернуться к использованию предыдущей версии баз,

1. Откройте главное окно приложения и выберите компонент **Обновление**.
2. Нажмите на ссылку Вернуться к предыдущим базам.

13.3. Настройка обновления

Обновление приложения выполняется в строгом соответствии с параметрами, определяющими:

- с какого ресурса производится копирование и установка обновлений приложения (см. п. 13.3.1 на стр. 161);
- в каком режиме запускается процесс обновления приложения и что именно обновляется (см. п. 13.3.2 на стр. 164);
- как часто требуется запускать обновление, в случае если настроен запуск по расписанию (см. п. 6.7 на стр. 67);
- от имени какой учетной записи будет выполнено обновление (см. п. 6.6 на стр. 65);
- требуется ли копировать полученные обновления в локальный каталог (см. п. 13.3.3 на стр. 165);
- какие действия нужно выполнять после обновления приложения (см. п. 13.3.3 на стр. 165).

В данном разделе Руководства будут детально рассмотрены все перечисленные выше аспекты.

13.3.1. Выбор источника обновлений

Источник обновлений – это некоторый ресурс, содержащий обновления баз и внутренних модулей Антивируса Касперского. Источником обновления могут быть http- или ftp-серверы, локальные или сетевые каталоги.

Основным источником для обновления являются *серверы обновлений «Лаборатории Касперского»*. Это специальные интернет-сайты, на которые выкладываются обновления баз и внутренних модулей для всех продуктов «Лаборатории Касперского».

В случае если у вас нет доступа к серверам обновлений «Лаборатории Касперского» (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.

Внимание!

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

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

Выбор источника обновлений производится на закладке **Источник обновлений** (см. рис. 52).

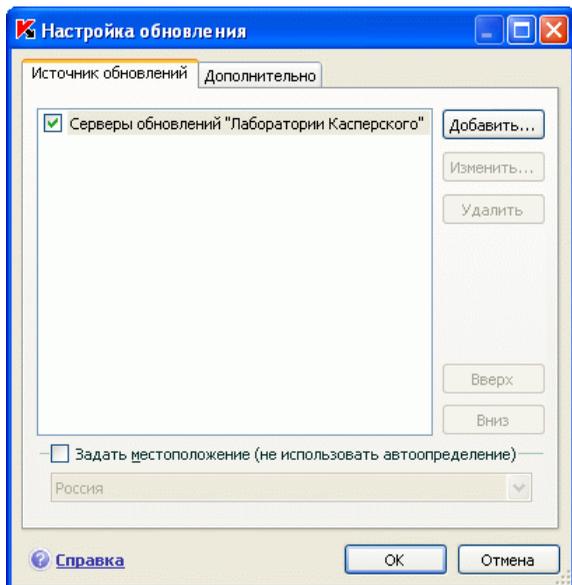


Рисунок 52. Выбор источника обновлений

По умолчанию список содержит только серверы обновлений «Лаборатории Касперского». Список серверов не доступен для редактирования. В процессе обновления Антивирус Касперского обращается к данному списку, выбирает первый по порядку адрес сервера и пытается загрузить с него обновления. Если выполнить обновление с выбранного адреса невозможно, приложение обращается к следующему по списку серверу и вновь пытается получить обновления. Адрес сервера, с которого будет произведено обновление, автоматически поместится в начало списка. При очередном обновлении с серверов «Лаборатории Касперского» приложение в первую очередь обратится именно к тому серверу, с которого в предыдущий раз было выполнено успешное обновление.

Чтобы обновление производилось с некоторого ftp-, http-сайта,

1. Нажмите на кнопку **Добавить**.
2. Выберите ftp-, http-сайт в окне **Выбор источника обновлений** или укажите его IP-адрес, символьное имя или url-адрес в поле **Источник**. При выборе в качестве источника обновлений некоторого ftp-ресурса допускается указание параметров авторизации в url-адресе сервера в формате `ftp://<имя_пользователя>:<пароль>@<хост>:<порт>`.

Внимание!

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

Чтобы обновлять приложение из некоторого каталога,

1. Нажмите на кнопку **Добавить**.
2. Выберите каталог в окне **Выбор источника обновлений** или введите полный путь к нему в поле **Источник**.

Антивирус Касперского добавляет новый источник обновлений в начало списка и автоматически включает его использование – устанавливает рядом с ним флажок.

Если в качестве источников обновлений выбрано несколько ресурсов, то в процессе обновления приложение обращается к ним строго по списку и обновляется с первого доступного источника. Вы можете поменять порядок следования источников в списке с помощью кнопок **Вверх / Вниз**.

Редактировать список источников вы можете по кнопкам **Добавить**, **Изменить**, **Удалить**. Серверы обновлений «Лаборатории Касперского» – это единственный источник, недоступный для редактирования и удаления.

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

Для выбора ближайшего сервера установите флажок **Задать местоположение (не использовать автоопределение)** и в раскрывающемся списке выберите ближайшую к вашему текущему местоположению страну. Если флажок установлен, то обновление будет производиться с учетом выбранного в списке региона. По умолчанию флажок снят и при обновлении используется информация о текущем регионе из реестра операционной системы.

13.3.2. Выбор режима и предмета обновления

Важным моментом в настройке обновления приложения является определение предмета обновления и режима обновления.

Предмет обновления (см. рис. 53) определяет, что именно будет обновляться:

- базы приложения;
- сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты;
- модули приложения.

Базы приложения и сетевые драйверы обновляются всегда, а программные модули только в том случае, если установлен соответствующий режим.

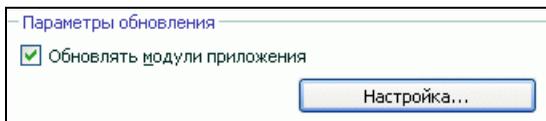


Рисунок 53. Выбор предмета обновления

Чтобы в процессе обновления на ваш компьютер копировались и устанавливались обновления модулей приложения,

откройте окно настройки приложения, выберите раздел обновление и установите флажок **Обновлять модули приложения**.

Если на данный момент в источнике присутствует обновление модулей приложения, на вашем экране будет открыто специальное окно, содержащее описание всех текущих изменений в модулях приложения. На основании такого описания вы сможете сделать вывод, требуется устанавливать данное обновление или нет.

Режим обновления приложения (см. рис. 54) определяет, каким образом будет производиться запуск обновления. Вы можете выбрать один из следующих режимов в блоке **Режим запуска**:

 **Автоматически**. Антивирус Касперского с заданной периодичностью проверяет наличие пакета обновлений в источнике обновлений (см. п. 13.3.1 на стр. 161). При обнаружении свежих обновлений приложение скачивает их и устанавливает на компьютер. Такой режим обновления используется по умолчанию.

Если в качестве источника выбран сетевой ресурс, Антивирус Касперского будет производить попытку обновления через интервал, указанный в предыдущем пакете обновлений. Из локального источника обновление производится с интервалом, указанным в предыдущем пакете обновлений. Такая возможность позволяет автоматически регулировать частоту обновлений в случае вирусных эпидемий и других опасных ситуаций. Приложение своевременно будет получать самые последние обновления баз и модулей приложения, что исключит возможность проникновения опасных программ на ваш компьютер.



Рисунок 54. Выбор режима запуска обновления

- **По расписанию.** Обновление приложения производится в соответствии с установленным графиком. Если вы хотите перейти на такой режим обновления, то по умолчанию вам будет предложено проводить обновление раз в день. Чтобы сформировать другое расписание, нажмите на кнопку **Изменить** рядом с названием режима и в открывшемся окне произведите соответствующие изменения (подробнее см. п. 6.7 на стр. 67).
- **Вручную.** В этом случае вы самостоятельно запускаете обновление приложения. Антивирус Касперского обязательно уведомит вас о необходимости обновления.

13.3.3. Копирование обновлений

Если домашние компьютеры объединены в локальную сеть, нет необходимости скачивать и устанавливать обновления на каждый из них отдельно, поскольку в этом случае увеличивается сетевой трафик. Вы можете воспользоваться сервисом копирования обновлений, который позволяет уменьшить трафик за счет того, что процедура получения обновлений организована следующим образом:

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

Для подключения сервиса копирования обновлений на закладке **Дополнительно** (см. рис. 55) установите флажок **Копировать в папку** и в поле

ниже укажите путь к папке общего доступа, куда будут помещаться полученные обновления. Путь можно ввести вручную либо выбрать в окне, открываемом по кнопке **Обзор**. Если флажок установлен, при получении новых обновлений они будут автоматически скопированы в данную папку.

Обратите внимание, что Антивирус Касперского 7.0 получает с серверов «Лаборатории Касперского» только собственный пакет обновлений.

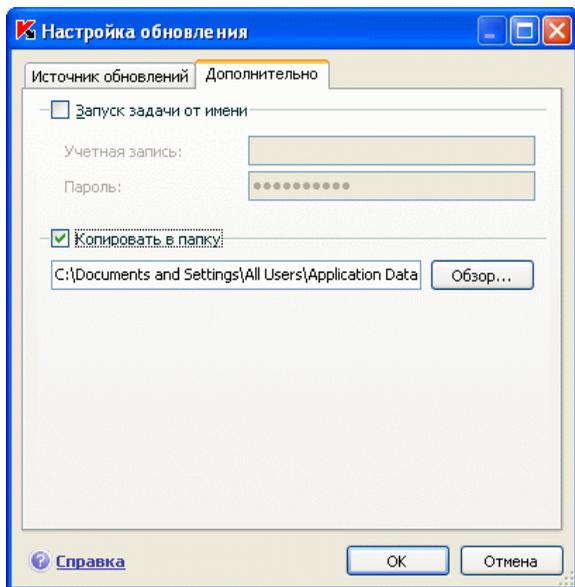


Рисунок 55. Настройка сервиса копирования обновлений

Для того чтобы другие компьютеры сети обновлялись из папки, содержащей скопированные из интернета обновления, необходимо выполнить следующие действия:

1. Открыть общий доступ к этой папке.
2. На компьютерах сети в настройках сервиса обновления указать папку общего доступа в качестве источника обновления.

13.3.4. Действия после обновления приложения

Каждое обновление баз приложения содержит в себе новые записи, позволяющие защищать ваш компьютер от появившихся недавно угроз.

Специалисты «Лаборатории Касперского» рекомендуют вам сразу после обновления приложения проверять *объекты, помещенные на карантин, и объекты автозапуска*.

Почему именно эти объекты?

На карантин помещаются объекты, при проверке которых не удалось точно определить, какими вредоносными программами они поражены (см. п. 15.1 на стр. 171). Возможно после обновления баз Антивирус Касперского сможет однозначно определить опасность и обезвредить ее.

По умолчанию приложение проверяет объекты на карантине после каждого обновления. Рекомендуем вам периодически просматривать объекты на карантине. В результате проверки у них может измениться статус. Ряд объектов можно будет восстановить в прежнее местоположение и продолжить работу с ними.

Чтобы отменить проверку объектов на карантине, снимите флажок  **Проверять файлы на карантине** в блоке **Действие после обновления**.

Объекты автозапуска являются критической областью в контексте безопасности вашего компьютера. Если данная область будет поражена вредоносной программой, то, возможно, вам даже не удастся загрузить операционную систему. Для проверки данной области в Антивирусе Касперского есть встроенная задача проверки объектов автозапуска (см. Глава 11 на стр. 136). Рекомендуем настроить автоматический режим запуска данной задачи после каждого обновления баз (см. п. 6.7 на стр. 67).

ГЛАВА 14. УПРАВЛЕНИЕ КЛЮЧАМИ

Возможность использования Антивируса Касперского определяется наличием *файла ключа*. Ключ предоставляется вам на основании покупки продукта и дает право использовать приложение со дня установки ключа.

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

Если была активирована пробная версия приложения, то после завершения срока ее использования, Антивирус Касперского работать не будет.

По окончании срока действия коммерческого ключа функциональность приложения сохраняется за исключением возможности обновления баз приложения. Вы по-прежнему можете проверять ваш компьютер посредством задач поиска вирусов и использовать компоненты защиты, но только на основе баз, актуальных на дату окончания срока действия ключа. 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 ключ на использование Антивируса Касперского. За две недели до истечения срока действия ключа приложение уведомляет вас об этом. В течение двух недель при каждом запуске приложения на экран выводится соответствующее сообщение.

Информация об используемом ключе представлена в разделе **Активация** (см. рис. 56) главного окна приложения. В блоке **Установленные ключи** указан номер ключа, его тип (коммерческий, пробный, для бета-тестирования), ограничение количества компьютеров, на которых можно использовать данный ключ, дата окончания срока действия ключа и количество дней до этой даты. Для просмотра дополнительной информации воспользуйтесь ссылкой [Посмотреть детальную информацию о ключах](#).

Чтобы ознакомиться с условиями лицензионного соглашения на использование приложения воспользуйтесь ссылкой [Просмотреть лицензионное соглашение](#). Для удаления ключа из списка нажмите на ссылку [Удалить](#).

Для приобретения ключа или продления срока его действия выполните следующее:

1. Приобретите новый ключ. Для этого воспользуйтесь ссылкой веб-[Приобрести новый ключ](#) (в случае если приложение не было активировано) или [Продлить срок действия ключа](#). На открывшейся

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 приложения.

2. Установите ключ. Для этого воспользуйтесь ссылкой **Установить ключ** в разделе **Активация** главного окна Антивируса Касперского либо командой **Активация** контекстного меню приложения. В результате будет запущен мастер активации (см. п. 3.2.2 на стр. 36).

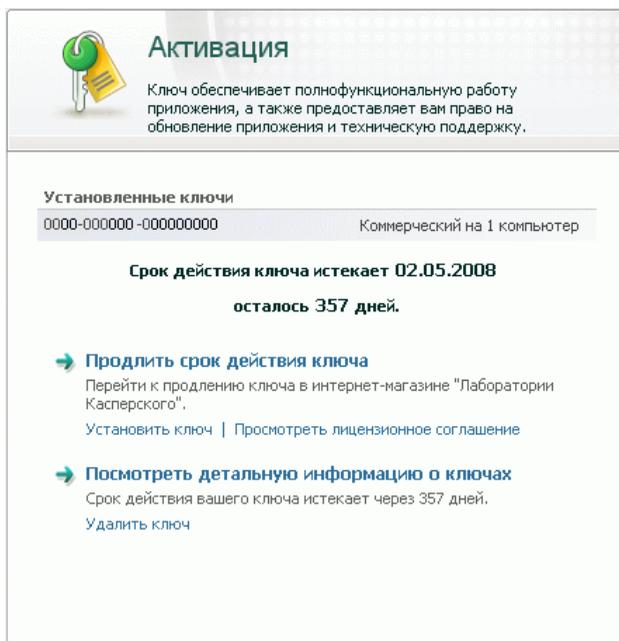


Рисунок 56. Управление ключами

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**.

ГЛАВА 15. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Помимо обеспечения защиты ваших данных приложение обладает дополнительными сервисами, расширяющими возможности работы с Антивирусом Касперского.

В процессе работы приложение помещает некоторые объекты в специальные хранилища. Цель, которая при этом преследуется, – обеспечить максимальную защиту данных с минимальными потерями.

- Резервное хранилище содержит копии объектов, которые были изменены или удалены в результате работы Антивируса Касперского (см. п. 15.2 на стр. 175). Если какой-либо объект содержал важную для вас информацию, которую не удалось полностью сохранить в процессе антивирусной обработки, вы всегда сможете восстановить объект из его резервной копии.
- Карантин содержит возможно зараженные объекты, которые не удалось обработать с помощью текущей версии баз приложения (см. п. 15.1 на стр. 171).

Рекомендуется периодически просматривать списки объектов, возможно некоторые из них уже неактуальны, а некоторые можно восстановить.

Часть сервисов направлена на помощь в работе с приложением, например:

- Сервис Службы технической поддержки обеспечивает всестороннюю помощь в работе с Антивирусом Касперского (см. п. 15.10 на стр. 206). Эксперты «Лаборатории Касперского» постарались включить все возможные способы обеспечения поддержки: он-лайн поддержка, форум пользователей, База знаний.
- Сервис уведомлений о событиях помогает настраивать оповещение пользователей о важных моментах в работе Антивируса Касперского (см. п. 15.9.1 на стр. 198). Это могут быть как события информационного характера, так и ошибки, которые требуют безотлагательного устранения, и знать о них крайне важно.
- Сервис самозащиты приложения и ограничения доступа к работе с ним обеспечивает защиту собственных файлов приложения от изменения и повреждения со стороны злоумышленников, запрещает внешнее управление сервисами приложения, а также вводит разграничение прав других пользователей вашего компьютера на выполнение некоторых действий с Антивирусом Касперского (см. п. 15.9.2

на стр. 201). Например, изменение уровня защиты может значительно повлиять на безопасность информации на вашем компьютере.

- Сервис управления конфигурацией приложения обеспечивает сохранение параметров работы приложения и перенесение их на другие компьютеры (см. п. 15.9.3 на стр. 204), а также восстановление параметров по умолчанию (см. п. 15.9.4 на стр. 205).

Также приложение предоставляет подробные отчеты (см. п. 15.3 на стр. 177) о работе всех компонентов защиты и выполнении всех задач поиска вирусов, обновления.

Формирование списка контролируемых портов позволяет регулировать контроль поступающей и передаваемой по ним информации некоторыми компонентами защиты Антивируса Касперского (см. п. 15.4 на стр. 185). Настройка параметров-прокси сервера (см. п. 15.7 на стр. 193) обеспечивает доступ приложения к интернету, что важно для работы некоторых компонентов постоянной защиты, и обновления.

Создание диска аварийного восстановления позволяет восстанавливать работоспособность компьютера на уровне, предшествующем заражению (см. п. 15.4 на стр. 185). Это особенно полезно в ситуации, когда после повреждения вредоносным кодом системных файлов невозможно произвести загрузку операционной системы компьютера.

Вам также предоставляется возможность изменять внешний вид Антивируса Касперского и настраивать параметры текущего интерфейса приложения (см. п. 15.7 на стр. 193).

Рассмотрим подробнее все перечисленные сервисы.

15.1. 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 приложения 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 изменен-

ной 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 приложения 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 поиска вирусов, а также Файловым Антивирусом, Почтовым Антивирусом и Проактивной защитой.

Вы сами можете поместить объект на карантин, воспользовавшись ссылкой Карантин в специальном уведомлении, которое открывается на экране вашего компьютера при обнаружении возможно зараженного объекта.

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.

15.1.1. Действия с объектами на карантине

Общее количество объектов, помещенных на карантин, приводится в разделе **Отчеты и файлы данных** главного окна приложения. В правой части главного окна есть специальный блок **Карантин**, отображающий:

- количество возможно зараженных объектов, обнаруженных в процессе работы Антивируса Касперского;
- текущий размер хранилища.

Здесь же можно удалить все объекты карантина по ссылке Очистить. Обратите внимание, что при этом будут также удалены объекты резервного хранилища и файлы отчетов.

Чтобы перейти к объектам на карантине,

воспользуйтесь ссылкой Карантин.

На закладке карантина (см. рис. 57) вы можете выполнять следующие действия:

- Переносить на карантин файл, подозреваемый вами на присутствие вируса, но не обнаруженный приложением. Для этого нажмите на кнопку **Добавить** и в стандартном окне выбора укажите нужный файл. Он будет добавлен в список со статусом *добавлен пользователем*.

Если вручную поместить на карантин файл, который при последующей проверке окажется незараженным, его статус после проверки не сразу будет изменен на *ок*. Это произойдет только если проверка производилась через некоторое время (не менее трех дней) после помещения файла на карантин.

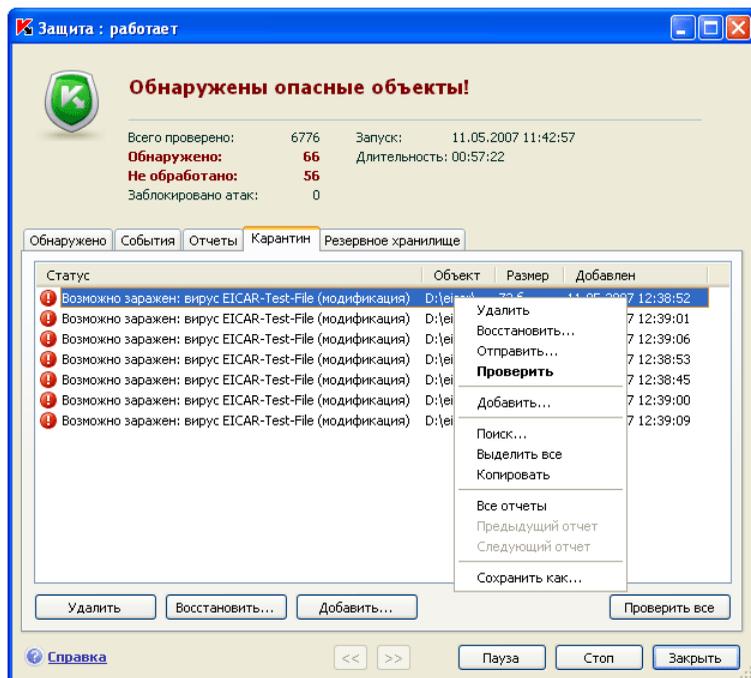


Рисунок 57. Список объектов на карантине

- Проверять и лечить с использованием текущей версии баз приложения все возможно зараженные объекты карантина. Для этого нажмите на кнопку **Проверить все**.

В результате проверки и лечения любого объекта карантина его статус может измениться на *заражен*, *возможно заражен*, *ложное срабатывание*, *ок* и др.

Статус объекта *заражен* означает, что объект был идентифицирован как зараженный, но вылечить его не удалось. Рекомендуем вам удалять объекты с таким статусом.

Все объекты со статусом *ложное срабатывание* можно безбоязненно восстанавливать, поскольку их предыдущий статус *возможно заражен* не был подтвержден приложением при повторной проверке.

- Восстанавливать файлы в каталог, заданный пользователем, или каталоги, откуда они были перенесены на карантин (по умолчанию). Для восстановления объекта выберите его в списке и нажмите на кнопку **Восстановить**. При восстановлении объектов, помещенных на карантин из архивов, почтовых баз и файлов почтовых форматов необходимо дополнительно указать каталог, в который они будут восстанавливаться.

Совет.

Рекомендуем вам восстанавливать только объекты со статусом *ложное срабатывание*, *ок*, *вылечен*, поскольку восстановление других объектов может привести к заражению вашего компьютера!

- Удалять любой объект карантина или группу выбранных объектов. Удаляйте только те объекты, которые невозможно вылечить. Для того чтобы удалить объекты, выберите их в списке и нажмите на кнопку **Удалить**.

15.1.2. Настройка параметров карантина

Вы можете настроить параметры формирования и работы карантина, а именно:

- Задать режим автоматической проверки объектов на карантине после каждого обновления баз приложения (подробнее см. п. 13.3.3 на стр. 165).

Внимание!

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

- Определить максимальный срок хранения объектов на карантине.

По умолчанию срок хранения объектов на карантине составляет 30 дней, по истечении которого объекты удаляются. Вы можете изменить максимальный срок хранения возможно зараженных объектов или отменить такое ограничение вообще.

Для этого:

1. Откройте окно настройки приложения и выберите раздел **Отчеты и файлы данных**.
2. В блоке **Карантин и Резервное хранилище** (см. рис. 58) укажите временной период, после которого объекты, находящиеся в хранилище, будут автоматически удалены.

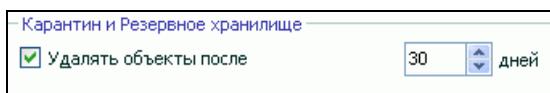


Рисунок 58. Настройка срока хранения объектов на карантине

15.2. Резервные копии опасных объектов

Иногда при лечении объектов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, и в результате лечения она стала недоступной полностью или частично, 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 – возможность в любой момент восстановить исходный объект. Файлы в резервном хранилище хранятся в специальном формате и не представляют опасности.

15.2.1. Действия с резервными копиями

Общее количество резервных копий объектов, помещенных в хранилище, приводится в разделе **Отчеты и файлы данных** главного окна приложения. В правой части главного окна есть специальный блок **Резервное хранилище**, отображающий:

- количество копий опасных объектов, созданных в процессе работы Антивируса Касперского;
- текущий размер хранилища.

Здесь же можно удалить все копии хранилища по ссылке Очистить. Обратите внимание, что при этом будут также удалены объекты карантина и файлы отчетов.

Чтобы перейти к копиям опасных объектов,

используйте ссылку Резервное хранилище.

В центральной части закладки (см. рис. 59) хранилища представлен список резервных копий. Для каждой копии приведена следующая информация: полное имя объекта с указанием пути к исходному местоположению, статус объекта, присвоенный по результатам проверки, и его размер.

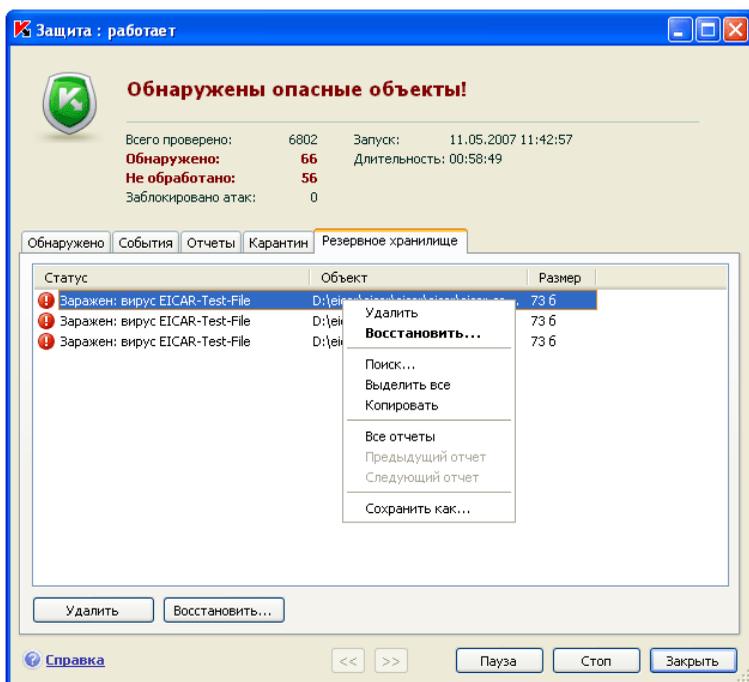


Рисунок 59. Резервные копии удаленных или вылеченных объектов

Вы можете восстановить выбранные копии с помощью кнопки **Восстановить**. Объект восстанавливается из резервного хранилища с тем же именем, которое было у него до лечения.

Если в исходном местоположении находится объект с таким именем (такая ситуация возможна при восстановлении объекта, копия которого была создана перед лечением), на экран будет выведено соответствующее предупреждение. Вы можете изменить местоположение восстанавливаемого объекта или переименовать его.

Рекомендуем вам сразу после восстановления проверить объект на присутствие вирусов. Возможно с обновленными базами приложения его удастся вылечить без потери целостности.

Не рекомендуем вам восстанавливать резервные копии объектов, если в этом нет большой необходимости. Это может привести к заражению компьютера.

Рекомендуем вам периодически просматривать хранилище и проводить его очистку с помощью кнопки **Удалить**. Вы также можете настроить приложение, чтобы оно самостоятельно удаляла наиболее старые копии из хранилища (см. п. 15.2.2 на стр. 177).

15.2.2. Настройка параметров резервного хранилища

Вы можете определить максимальный срок хранения копий в резервном хранилище.

По умолчанию срок хранения копий опасных объектов составляет 30 дней, по истечении которого копии удаляются. Вы можете изменить максимальный срок хранения копий или снять такое ограничение вообще. Для этого:

1. Откройте окно настройки приложения и выберите раздел **Отчеты и файлы данных**.
2. Настройте срок хранения резервных копий в хранилище в блоке **Карантин и Резервное хранилище** (см. рис. 58) правой части окна.

15.3. Отчеты

Работа каждого компонента Антивируса Касперского и выполнение каждой задачи поиска вирусов и обновления фиксируется в отчете.

Общее количество отчетов, сформированных приложением на текущий момент времени, а также их общий размер в байтах отражены разделе **Отчеты и файлы данных** главного окна приложения. Данная информация приведена в блоке **Отчеты**.

Чтобы перейти к просмотру отчетов, воспользуйтесь ссылкой [Отчеты](#).

В результате будет открыто окно на закладке **Отчеты** (см. рис. 60). Здесь приведены последние отчеты по всем компонентам, задачам поиска вирусов и обновления, запущенным в текущей сессии работы Антивируса Касперского. Напротив каждого компонента или задачи указан результат работы. Например, *работает*, *пауза* или *выключен*. Если вы хотите просмотреть полную историю формирования отчетов текущей сессии работы приложения, установите флажок **Показывать историю отчетов**.

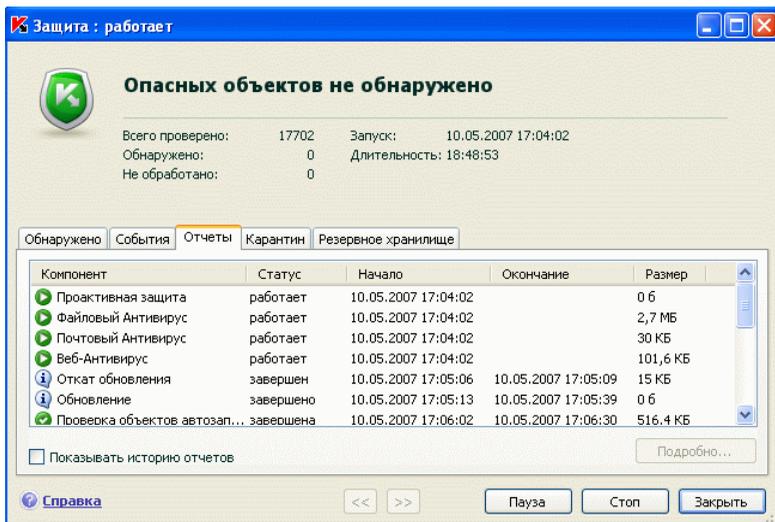


Рисунок 60. Отчеты о работе компонентов приложения

Чтобы ознакомиться со всеми событиями, зафиксированными в отчете о работе компонента или выполнении задачи,

выберите имя компонента или задачи на закладке **Отчеты** и нажмите на кнопку **Подробнее**.

В результате будет открыто окно, содержащее детальную информацию о работе выбранного компонента или задачи. Результирующая статистика работы приведена в верхней части окна, а подробная информация размещена на разных закладках в центральной части. В зависимости от компонента или задачи состав закладок может быть разным:

- Закладка **Обнаружено** содержит список опасных объектов, обнаруженных в результате работы компонента или выполненной задачи поиска вирусов.

- Закладка **События** отражает все события в работе компонента или задачи.
- Закладка **Статистика** включает подробную статистику всех проверенных объектов.
- Закладка **Параметры** отображает набор параметров, в соответствии с которыми работает компонент защиты, задача поиска вирусов или обновление баз приложения.
- Закладка **Реестр** присутствует только в отчете проактивной защиты и содержит информацию о всех попытка изменения системного реестра операционной системы.

Весь отчет вы можете импортировать в текстовый файл. Например, это полезно в том случае, если в работе компонента или при выполнении задачи возникла ошибка, устранить которую самостоятельно вы не можете, и требуется помощь Службы технической поддержки. В этом случае отчет в текстовом формате необходимо отправить в Службу поддержки, чтобы наши специалисты могли детально изучить проблему и решить ее как можно скорее.

Для того чтобы импортировать отчет в текстовый файл,

нажмите на кнопку **Действия**→**Сохранить как** и укажите, куда бы вы хотели сохранить файл отчета.

По завершении работы с отчетом нажмите на кнопку **Заккрыть**.

На всех закладках отчета кроме **Параметров** и **Статистики** расположена кнопка **Действия**, по которой вы можете произвести ряд действий над объектами списка. По этой кнопке открывается контекстное меню со следующими пунктами (в зависимости от компонента, отчет по которому вы просматриваете, список пунктов меню отличается, ниже приведены все возможные пункты):

Лечить – произвести попытку лечения опасного объекта. Если обезвредить объект не получится, вы можете оставить его в этом списке для отложенной проверки с обновленными базами приложения или удалить. Вы можете применить данное действие как к одному объекту списка, так и к нескольким выбранным объектам.

Удалить – удалить опасный объект с компьютера.

Удалить из списка – удалить запись об обнаружении объекта из отчета.

Добавить в доверенную зону – добавить объект как исключение из защиты. При этом будет открыто окно с правилом исключения для данного объекта.

Лечить все – обезвредить все объекты списка. Антивирус Касперского попытается обработать объекты с использованием баз приложения.

Очистить – удалить все опасные объекты без попытки их лечения.

Показать файл – открыть Microsoft Windows Explorer на каталоге, где расположен данный объект.

Посмотреть на www.viruslist.ru – перейти к описанию объекта в Вирусной энциклопедии на сайте «Лаборатории Касперского».

Поиск – задать условия поиска по имени объекта или статусу.

Сохранить как – сохранить отчет в текстовом формате.

Кроме того, вы можете сортировать информацию, представленную в окне, по возрастанию и убыванию каждого из столбцов.

Обработка опасных объектов, обнаруженных в ходе работы Антивируса Касперского, выполняется с помощью кнопок **Лечить** (для одного объекта или группы выбранных объектов) или **Лечить все** (для обработки всех объектов списка). При обработке каждого объекта на экран будет выведено уведомление, где вам будет необходимо принять решение о дальнейших действиях над ним.

Если в окне уведомления вы установите флажок **Применить во всех подобных случаях**, то выбранное действие будет применено ко всем объектам с тем же статусом, выбранным в списке перед началом обработки.

15.3.1. Настройка параметров отчетов

Для настройки параметров формирования и хранения отчетов:

1. Откройте окно настройки приложения и выберите раздел **Отчеты и файлы данных**.
2. В блоке **Отчеты** (см. рис. 61) произведите необходимую настройку:
 - разрешите или запретите запись в отчет событий информационного характера. Как правило, такие события не являются важными для обеспечения защиты. Для того чтобы разрешить запись, установите флажок **Записывать не критические события**;
 - включите хранение в отчете только событий, произошедших при последнем запуске задачи. Это позволит сэкономить место на диске за счет уменьшения размера отчета. Если флажок **Хранить только текущие события** установлен, информация, представленная в отчете, будет обновляться при каждом перезапуске задачи. Однако перезаписи подлежит только информация не критического характера.

- установите срок хранения отчетов. По умолчанию срок хранения отчетов составляет 30 дней, по истечению которого отчеты удаляются. Вы можете изменить максимальный срок хранения или отменить такое ограничение вообще.

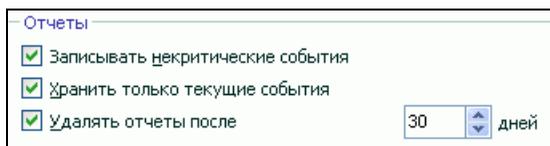


Рисунок 61. Настройка параметров формирования отчетов

15.3.2. Закладка **Обнаружено**

Данная закладка (см. рис. 62) содержит список опасных объектов, обнаруженных Антивирусом Касперского. Для каждого объекта указывается его полное имя и статус, присвоенный приложением при его проверке / обработке.

Чтобы список содержал не только опасные объекты, но и те, что были успешно обезврежены, установите флажок **Показывать вылеченные объекты**.

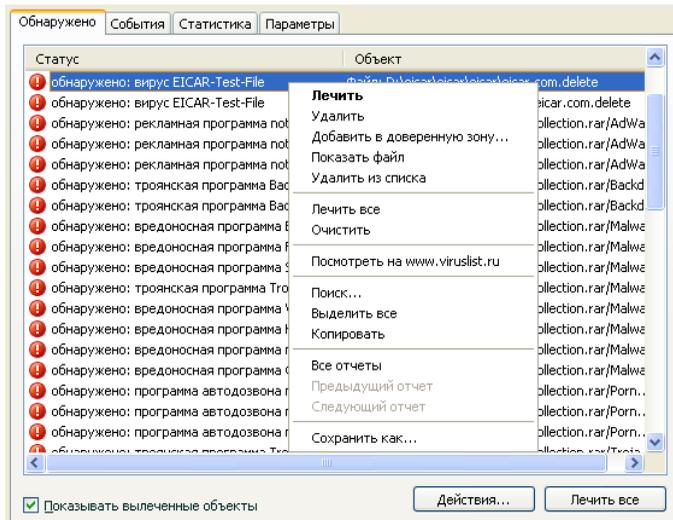


Рисунок 62. Список обнаруженных опасных объектов

Обработка опасных объектов, обнаруженных в ходе работы Антивируса Касперского, выполняется с помощью кнопок **Лечить** (для одного объекта

или группы выбранных объектов) или **Лечить все** (для обработки всех объектов списка). При обработке каждого объекта на экран будет выведено уведомление, где вам будет необходимо принять решение о дальнейших действиях над ним.

Если в окне уведомления вы установите флажок **Применить во всех подобных случаях**, то выбранное действие будет применено ко всем объектам с тем же статусом, выбранным в списке перед началом обработки.

15.3.3. Закладка *События*

Полный список всех важных событий в работе компонента защиты или при выполнении задачи поиска вирусов либо обновления фиксируется на данной закладке (см. рис. 63), если это не было отменено правилом контроля активности (см. п. 10.1 на стр. 123).

События могут быть следующих типов:

Критические события – события критической важности, указывающие на проблемы в работе приложения или на уязвимости в защите вашего компьютера. Например, *обнаружен вирус, сбой в работе*.

Важные события – события, на которые обязательно нужно обратить внимание, поскольку они отображают важные ситуации в работе приложения. Например, *прервано пользователем*.

Информационные события – события справочного характера, как правило, не несущие важной информации. Например, *ок, не обработан*. Данные события отображаются в журнале событий только в том случае, если установлен флажок **Показывать все события**.

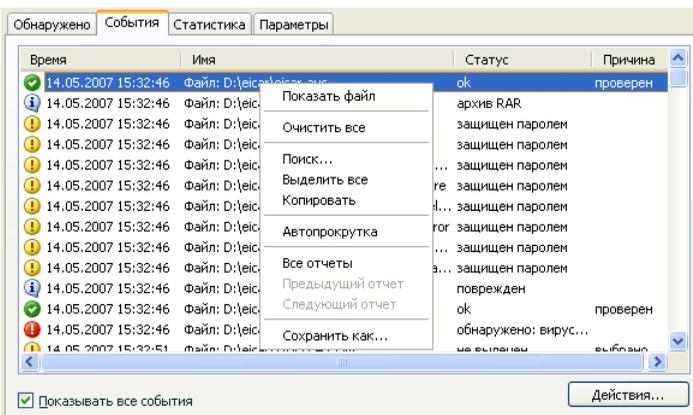


Рисунок 63. События, возникшие в работе компонента

Формат представления событий в журнале событий может различаться в зависимости от компонента или задачи. Так, для задачи обновления приводится:

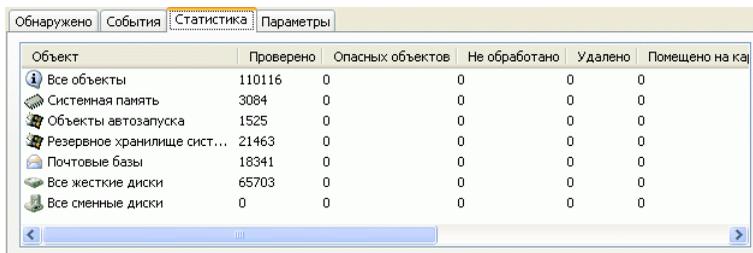
- название события;
- имя объекта, для которого зафиксировано это событие;
- время, когда произошло событие;
- размер загружаемого файла.

Для задачи поиска вирусов журнал событий содержит имя проверяемого объекта и статус, присвоенный объекту в результате проверки / обработки.

15.3.4. Закладка *Статистика*

Подробная статистика работы компонента или выполнения задачи поиска вирусов фиксируется на данной закладке (см. рис. 64). Здесь вы можете узнать:

- Сколько объектов было проверено на наличие опасных объектов в текущем сеансе работы компонента или при выполнении задачи. В том числе указано количество проверенных архивов, упакованных файлов, защищенных паролем и поврежденных объектов.
- Сколько было обнаружено опасных объектов, сколько из них не вылечено, удалено и помещено на карантин.



Объект	Проверено	Опасных объектов	Не обработано	Удалено	Помещено на кар
Все объекты	110116	0	0	0	0
Системная память	3084	0	0	0	0
Объекты автозапуска	1525	0	0	0	0
Резервное хранилище сист...	21463	0	0	0	0
Почтовые базы	18341	0	0	0	0
Все жесткие диски	65703	0	0	0	0
Все сменные диски	0	0	0	0	0

Рисунок 64. Статистика работы компонента

15.3.5. Закладка *Параметры*

Полный обзор параметров, в соответствии с которым работает компонент защиты, выполняется задача поиска вирусов или обновление приложения, приводится на закладке **Параметры** (см. рис. 65). Вы можете узнать, какой уровень защиты обеспечивает работа компонента, на каком уровне выполняется поиск вирусов, какое действие выполняется над опасным объектом

или какие параметры используются при обновлении приложения и т.д. Чтобы перейти к настройке параметров, воспользуйтесь ссылкой [Изменить параметры](#).

Для задач поиска вирусов вы можете настроить дополнительные условия выполнения:

- Установить приоритет выполнения задачи проверки при нагрузке на процессор. По умолчанию флажок **Уступать ресурсы другим приложениям** установлен. При этом приложение отслеживает уровень загрузки процессора и дисковых подсистем на предмет активности других приложений. Если уровень нагрузки существенно увеличивается и мешает нормальной работе приложений пользователя, приложение сокращает активность выполнения задач проверки. Это ведет к увеличению времени проверки и передаче ресурсов приложениям пользователя.
- Установить режим работы компьютера после завершения задачи проверки на вирусы. Вы можете настроить выключение / перезагрузку компьютера либо переход в режим ожидания или спящий режим. Для выбора варианта щелкните левой клавишей мыши по гиперссылке пока она не примет нужное значение.

Такая возможность полезна, например, если вы запускаете проверку компьютера на вирусы в конце рабочего дня и не хотите ждать ее завершения.

Однако использование этого параметра требует следующей дополнительной подготовки: нужно до запуска проверки отключить запрос пароля при проверке объектов, если он был включен, установить режим автоматической обработки опасных объектов. В результате выполненных действий интерактивный режим работы приложения отключается. Приложение не будет задавать вопросов, требующих ответов от вас и прерывающих процесс проверки.

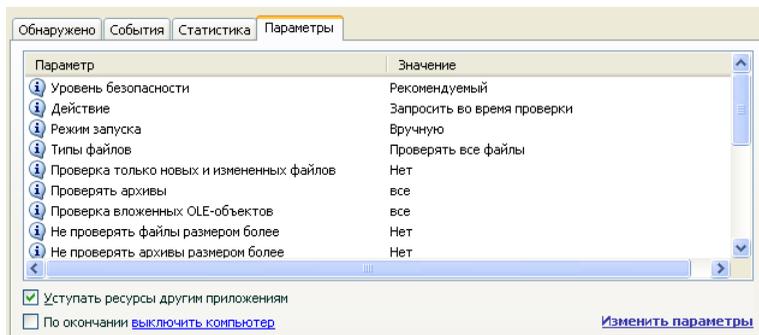
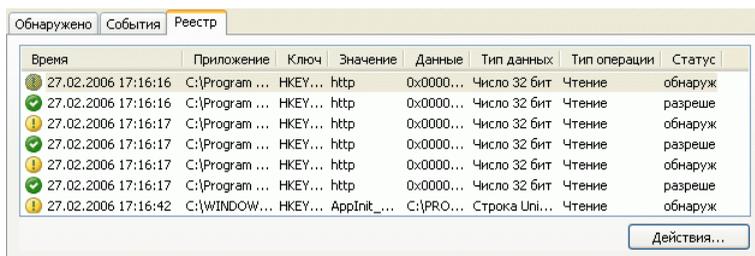


Рисунок 65. Параметры работы компонента

15.3.6. Закладка *Реестр*

Операции с ключами реестра, попытка которых была произведена с момента запуска приложения, фиксируются на закладке **Реестр** (см. рис. 66), если протоколирование не запрещено правилом (см. п. 10.3.2 на стр. 134).

На закладке приводится полное имя ключа, его значение, тип данных, а также сведения о производимой операции: попытка выполнения какого действия была произведена, в какое время и была ли она разрешена.



Время	Приложение	Ключ	Значение	Данные	Тип данных	Тип операции	Статус
27.02.2006 17:16:16	C:\Program ...	HKEY... http	0x0000...	Число 32 бит	Чтение	обнаруж	
27.02.2006 17:16:16	C:\Program ...	HKEY... http	0x0000...	Число 32 бит	Чтение	разреше	
27.02.2006 17:16:17	C:\Program ...	HKEY... http	0x0000...	Число 32 бит	Чтение	обнаруж	
27.02.2006 17:16:17	C:\Program ...	HKEY... http	0x0000...	Число 32 бит	Чтение	разреше	
27.02.2006 17:16:17	C:\Program ...	HKEY... http	0x0000...	Число 32 бит	Чтение	обнаруж	
27.02.2006 17:16:17	C:\Program ...	HKEY... http	0x0000...	Число 32 бит	Чтение	разреше	
27.02.2006 17:16:42	C:\WINDOW...	HKEY... AppInit_...	C:\PRO...	Строка Uni...	Чтение	обнаруж	

Рисунок 66. События по чтению и изменению системного реестра

15.4. Диск аварийного восстановления

В приложении Антивирус Касперского реализован сервис создания диска аварийного восстановления.

Диск аварийного восстановления предназначен для восстановления работоспособности системы после вирусной атаки, в результате которой повреждены системные файлы операционной системы и невозможна ее первоначальная загрузка. Этот диск включает:

- системные файлы Microsoft Windows XP Service Pack 2;
- набор утилит для диагностики операционной системы;
- файлы приложения Антивируса Касперского;
- файлы, содержащие базы приложения.

Чтобы создать диск аварийного восстановления:

1. Откройте главное окно приложения и выберите раздел **Поиск вирусов**.
2. Нажмите на ссылку Создать диск аварийного восстановления для начала процесса создания диска.

Диск аварийного восстановления предназначен для того компьютера, на котором он был создан. Использование диска на других компьютерах может привести к непредсказуемым последствиям, поскольку на нем содержится информация о параметрах конкретного компьютера (например, информация о boot-секторах).

Создание диска аварийного восстановления доступно только в приложении, установленном на компьютере под управлением операционной системы Microsoft Windows XP и Microsoft Windows Vista. На компьютерах под управлением других поддерживаемых систем, в том числе и Microsoft Windows XP Professional x64 Edition и Microsoft Windows Vista x64, создание диска не предусмотрено.

15.4.1. Создание диска аварийного восстановления

Внимание! Для создания диска аварийного восстановления вам потребуется установочный диск Microsoft Windows XP Service Pack 2.

Диск аварийного восстановления создается с помощью специальной программы **PE Builder**.

Для создания диска с помощью PE Builder требуется предварительно установить эту программу на компьютер.

Создание диска аварийного восстановления сопровождается специальным мастером, который 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**.

Шаг 1. Подготовка к записи

Для создания диска аварийного восстановления укажите пути к следующим каталогам:

- Каталог установки программы PE Builder.
- Каталог хранения файлов диска аварийного восстановления перед записью на CD/DVD-диск.

Если вы создаете диск не впервые, данный каталог уже содержит набор файлов, подготовленных в предыдущий раз. Чтобы использо-

вать ранее сохраненные файлы, установите соответствующий флажок.

Обратите внимание, что ранее подготовленная версия файлов диска аварийного восстановления содержит старую версию баз приложения. Чтобы обеспечить оптимальный анализ компьютера на вирусы и восстановление системы, рекомендуется обновить базы и создать новую версию диска аварийного восстановления.

- Установочному диску Microsoft Windows XP Service Pack 2.

После ввода путей к требующимся каталогам нажмите на кнопку **Далее**. В результате будет запущена программа PE Builder и начнется процесс формирования файлов диска аварийного восстановления. Дождитесь завершения процесса, это может занять несколько минут.

Шаг 2. Создание ISO-файла

После завершения процесса формирования файлов диска аварийного восстановления программой PE Builder будет открыто окно **Создание ISO-файла**.

ISO-файл – это образ будущего диска в виде архива. Файлы iso-формата корректно воспринимаются большинством программ записи CD/DVD-дисков (например, Nero).

Если вы создаете диск аварийного восстановления не впервые, вы можете выбрать использование ISO-файла предыдущей версии. Для этого выберите вариант **Существующий ISO-файл**.

Шаг 3. Запись диска

В данном окне мастера вам предлагается указать, когда произвести запись файлов диска аварийного восстановления на CD/DVD-диск: в данный момент или позже.

Если вы выбрали немедленную запись диска, укажите, нужно ли очистить содержимое CD/DVD-носителя перед записью. Для этого установите соответствующий флажок. Данная возможность доступна только в случае, если CD/DVD-носитель поддерживает многократную перезапись данных (CD/DVD-RW).

При нажатии на кнопку **Далее** начнется процесс записи CD/DVD-диска. Дождитесь завершения процесса, это может занять несколько минут.

Шаг 4. Завершение создания диска аварийного восстановления

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

15.4.2. Использование диска аварийного восстановления

Обратите внимание, что в режиме аварийного восстановления Антивируса Касперского работает, только если запущено главное окно. При закрытии главного окна приложение будет выгружена.

В программе Bart PE, установленной по умолчанию, отсутствует поддержка `chm`-файлов и интернет-браузеров, поэтому в режиме аварийного восстановления недоступны просмотр справочной системы Антивируса Касперского, а также ссылки в интерфейсе приложения.

При возникновении ситуации, когда в результате вирусной атаки невозможно загрузить операционную систему, выполните следующие действия:

1. Создайте диск аварийного восстановления, используя приложение Антивирус Касперского на незараженном компьютере.
2. Вставьте диск аварийного восстановления в дисковод зараженного компьютера и перезагрузитесь. В результате будет запущена операционная система Microsoft Windows XP Service Pack 2 с интерфейсом программы Bart PE.

Программа Bart PE имеет встроенную сетевую поддержку для использования локальной сети. При запуске программы на экран будет выведен запрос на ее включение. Согласитесь с включением сетевой поддержки, если перед проверкой компьютера вы планируете обновить базы приложения из локальной сети. Если обновление не требуется, отмените включение сетевой поддержки.

3. Для запуска Антивируса Касперского выполните команду **GO** → **Programs** → **Kaspersky Anti-Virus 7.0** → **Start**.

В результате будет запущено главное окно Антивируса Касперского. В режиме аварийного восстановления доступны только задачи поиска вирусов и обновление баз приложения из локальной сети (в случае, если включена сетевая поддержка Bart PE).

4. Запустите проверку компьютера на вирусы.

Обратите внимание, что для проверки по умолчанию используются базы приложения, актуальные на дату создания диска аварийного восстановления. Поэтому перед началом проверки рекомендуется обновить базы.

Также обращаем внимание, что обновленные базы приложения будут использоваться приложением только в текущем сеансе работы с диском аварийного восстановления, до перезагрузки компьютера.

Внимание!

Если при проверке компьютера были обнаружены зараженные или возможно зараженные объекты, и была проведена их обработка с последующим помещением на карантин и в резервное хранилище, рекомендуется завершить обработку данных объектов в текущем сеансе работы с диском аварийного восстановления.

В противном случае данные объекты будут утрачены после перезагрузки компьютера.

15.5. Формирование списка контролируемых портов

В работе таких компонентов защиты как Почтовый Антивирус, Веб-Антивирус, контролируются потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые порты вашего компьютера. Так, например, Почтовый Антивирус анализирует информацию, передаваемую по SMTP-протоколу, Веб-Антивирус – HTTP-пакеты.

Список портов, которые обычно используются для передачи почты и HTTP-трафика, включен в поставку приложения. Вы можете добавить новый порт или отключить контроль некоторого порта, тем самым, отказавшись от анализа трафика, проходящего через данный порт, на присутствие опасных объектов.

Для редактирования списка контролируемых портов выполните следующие действия:

1. Откройте окно настройки приложения и выберите раздел **Контроль трафика**.
2. Нажмите на кнопку **Настройка портов**.
3. Откорректируйте список контролируемых портов в окне **Настройка портов** (см. рис. 67).

В данном окне представлен список портов, контролируемых Антивирусом Касперского. Для того чтобы проверять потоки данных, поступающих по всем открытым портам сети, выберите вариант  **Контролировать все**

порты. Для редактирования списка контролируемых портов вручную выберите вариант  **Контролировать только выбранные порты.**

Так, чтобы добавить новый порт в список контролируемых,

1. Нажмите на кнопку **Добавить** в окне настройки портов.
2. Номер порта и его описание введите в соответствующих полях окна **Новый порт.**

Например, на вашем компьютере есть нестандартный порт, через который настроен обмен данными с удаленным компьютером по HTTP-протоколу. Контроль HTTP-трафика осуществляется компонентом Веб-Антивирус. Для того чтобы анализировать данный трафик на присутствие вредоносного кода, вам нужно добавить этот порт в список контролируемых.

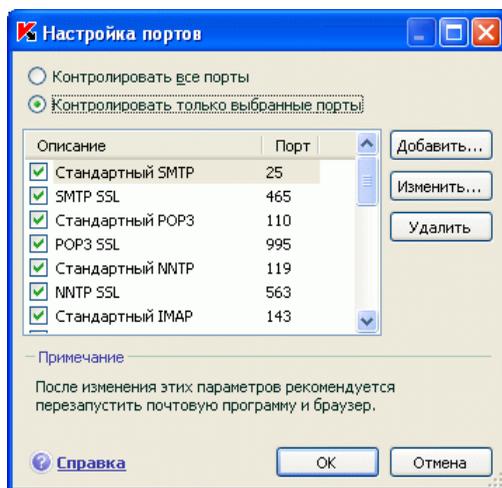


Рисунок 67. Список контролируемых портов

При запуске любого из компонентов Антивирус Касперского открывает на прослушивание всех входящих соединений порт 1110. В случае если данный порт в этот момент занят каким-либо приложением, для прослушивания выбирается порт 1111, 1112 и т. д.

Если вы одновременно пользуетесь Антивирусом Касперского и сетевым экраном (firewall) другой компании-производителя, требуется в параметрах этого сетевого экрана создать разрешающие правила для процесса `avp.exe` (внутренний процесс Антивируса Касперского) на всех перечисленных портах.

Например, в вашем сетевом экране создано правило для процесса *iexplorer.exe*, согласно которому данному процессу разрешено устанавливать соединения на порту 80.

Однако Антивирус Касперского, перехватывая запрос на соединение, инициируемое процессом *iexplorer.exe* на порту 80, передает его процессу *avr.exe*, который, в свою очередь, пытается самостоятельно установить соединение с запрашиваемой веб-страницей. Если для процесса *avr.exe* отсутствует разрешающее правило, сетевой экран заблокирует этот запрос. В результате веб-страница будет недоступна пользователю.

15.6. Проверка защищенных соединений

Соединение с использованием протокола SSL обеспечивает защиту канала обмена данными в интернете. Протокол SSL позволяет идентифицировать обменивающиеся данными стороны на основе электронных сертификатов, осуществлять шифрование передаваемых данных и обеспечивать их целостность в процессе передачи.

Эти особенности протокола используются злоумышленниками для распространения вредоносных программ, поскольку большинство антивирусных продуктов не проверяет SSL-трафик.

Антивирус Касперского предоставляет возможность проверки на вирусы трафика по протоколу SSL. При попытке соединения с веб-ресурсом в безопасном режиме на экран будет выведено уведомление (см. рис. 68) с запросом действия у пользователя.

В уведомлении приведена информация о программе, инициирующей соединение в безопасном режиме, а также удаленные адрес и порт. Вам предлагается принять решение о необходимости проверки на вирусы данного соединения:

- **Обработать** – выполнить проверку трафика на вирусы при соединении с веб-ресурсом в безопасном режиме.

Мы рекомендуем вам обязательно выполнять проверку SSL-трафика в случае, если вы находитесь на подозрительном веб-ресурсе и при переходе на следующую страницу начинается передача данных по SSL. С большой степенью вероятности это может быть признаком передачи вредоносной программы по защищенному протоколу.

- **Пропустить** – продолжить соединение с веб ресурсом в безопасном режиме без проверки трафика на вирусы.

Чтобы в дальнейшем применять выбранное действие ко всем попыткам установки SSL-соединений, установите флажок **Применить ко всем**.

Для проверки зашифрованных соединений Антивирус Касперского подменяет запрашиваемый сертификат безопасности самоподписным сертификатом. В некоторых случаях программы, устанавливающие соединение, отказываются принимать этот сертификат, в результате чего соединение не может быть установлено. Мы рекомендуем отключать проверку SSL-трафика в следующих случаях:

- При соединении с доверенным веб-ресурсом, например, с веб-страницей вашего банка, где вы осуществляете управление личным счетом. В этом случае важно получить подтверждение подлинности сертификата банка.
- Если программа, устанавливающая соединение, осуществляет проверку сертификата у запрашиваемого веб-ресурса. Например, программа MSN Messenger при установке защищенного соединения с сервером проверяет подлинность цифровой подписи Microsoft Corporation.

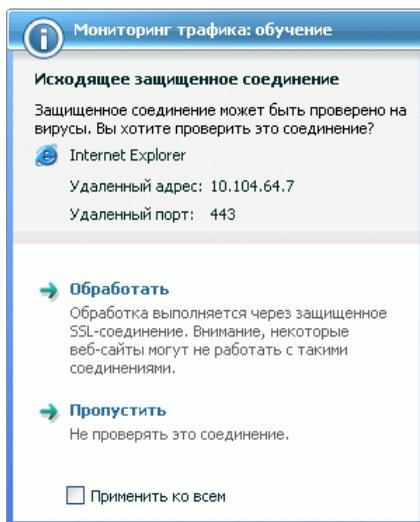


Рисунок 68. Уведомление об обнаружении SSL-соединения

Настройка проверки SSL-соединения выполняется в разделе **Контроль трафика** окна настройки приложения (см. рис. 69):

Проверять все защищенные соединения – проверять весь трафик, проходящий по протоколу SSL, на вирусы.

Запрашивать о проверке при обнаружении нового защищенного соединения – выводить сообщение с запросом действий пользователя при каждой попытке установки SSL-соединения.

Не проверять защищенные соединения – не проверять на вирусы трафик, проходящий по протоколу SSL.

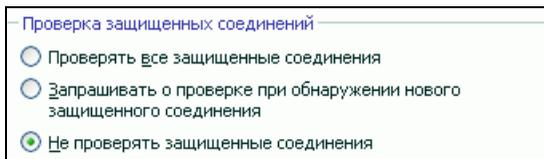


Рисунок 69. Настройка проверки защищенных соединений

15.7. Настройка параметров прокси-сервера

В разделе **Прокси-сервер** (см. рис. Рисунок 70) окна настройки приложения вы можете настроить параметры подключения к прокси-серверу (если выход в интернет осуществляется через прокси). Антивирус Касперского использует данные параметры в работе некоторых компонентов постоянной защиты, а также для обновления баз и модулей приложения.

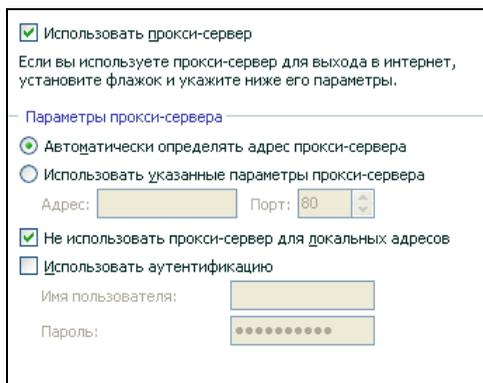


Рисунок 70. Настройка параметров прокси-сервера

Если для выхода в интернет используется прокси-сервер, установите флажок **Использовать прокси-сервер** и при необходимости настройте следующие параметры:

- Выберите, какие параметры прокси-сервера нужно использовать:

Автоматически определять адрес прокси-сервера. При выборе данного варианта параметры прокси-сервера определяются автоматически с помощью протокола WPAD (Web Proxy Auto-Discovery Protocol). В случае если по данному протоколу

определить адрес не удастся, Антивирус Касперского использует параметры прокси-сервера, указанные в Microsoft Internet Explorer.

- Использовать указанные параметры прокси-сервера** – использовать прокси-сервер, отличный от заданного в параметрах соединения браузера. В поле **Адрес** введите IP-адрес или символьное имя, а в поле **Порт** – порт прокси-сервера.

Для того чтобы при обновлении из локального или сетевого каталога не использовать прокси-сервер, установите флажок **Не использовать прокси-сервер для локальных адресов**.

- Укажите, используется ли аутентификация на прокси-сервере. *Аутентификация* – это процедура проверки регистрационных данных пользователя в целях контроля доступа.

Если для соединения с прокси необходимо пройти аутентификацию, установите флажок **Использовать аутентификацию** и укажите в приведенных ниже полях имя пользователя и пароль. В данном случае вначале будет проведена попытка NTLM-, а затем BASIC-авторизации.

В случае если флажок не установлен или данные не указаны, будет выполнена попытка NTLM-авторизации с использованием учетной записи, от имени которой запущена задача (например, обновление, см. п. 6.6 на стр. 65).

Если авторизация на прокси-сервере необходима, а вы не указали имя и пароль, или указанные данные по каким-либо причинам не были приняты прокси-сервером, будет открыто окно запроса имени и пароля авторизации. Если авторизация пройдет успешно, указанные имя и пароль будут использованы в дальнейшем. В противном случае, параметры авторизации будут запрошены повторно.

В случае обновления с ftp-сервера по умолчанию устанавливается соединение с сервером в пассивном режиме. При ошибке данного соединения выполняется попытка соединения в активном режиме.

По умолчанию время, отведенное на соединение с сервером обновления, составляет одну минуту. Если соединение не произошло, по истечении данного времени предпринимается попытка соединения со следующим сервером обновлений. Перебор производится до тех пор, пока процесс соединения не завершится успешно, или пока не будут перебраны все доступные серверы обновлений.

15.8. Настройка интерфейса Антивируса Касперского

Антивирус Касперского предоставляет вам возможность изменять внешний вид приложения, создавая и используя различные графические элементы и цветовую палитру. Также предполагается возможность настройки использования активных элементов интерфейса, таких как значок приложения в системной панели и всплывающие сообщения.

Для настройки интерфейса Антивируса Касперского:

откройте окно настройки приложения и выберите раздел **Вид** (см. рис. Рисунок 70).

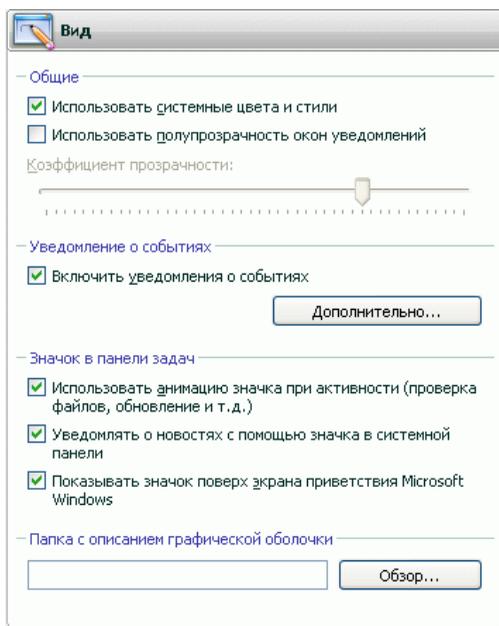


Рисунок 71. Настройка параметров интерфейса приложения

В правой части окна настройки вы можете определить:

- *Использование собственных графических элементов и цветовой палитры в интерфейсе приложения.*

По умолчанию в графической оболочке приложения используются системные цвета и стили. Вы можете отказаться от них, сняв флажок

Использовать системные цвета и стили. В этом случае будут использоваться стили, указанные вами при настройке темы экрана.

Все используемые в интерфейсе Антивируса Касперского цвета, шрифты, пиктограммы, тексты могут быть изменены. Вы можете создавать собственные графические оболочки для приложения, можете локализовать ее на другой язык. Чтобы подключить графическую оболочку, укажите каталог с ее параметрами в поле **Папка с описанием графической оболочки**. Для выбора каталога воспользуйтесь кнопкой **Обзор**.

- *Степень прозрачности всплывающих сообщений.*

Все операции Антивируса Касперского, требующие вашего немедленного уведомления или принятия решения, оформлены в виде всплывающих сообщений над значком приложения в системной панели. Окна сообщений полупрозрачны, чтобы не мешать вашей работе. При наведении на окно сообщения курсора мыши прозрачность исчезает. Вы можете менять степень прозрачности таких сообщений. Для этого установите ползунок шкалы **Коэффициент прозрачности** в нужное положение. Чтобы отменить прозрачность сообщений, снимите флажок **Использовать полупрозрачность окон уведомлений**.

- *Использовать или нет анимацию значка приложения в системной панели.*

В зависимости от выполняемой приложением операции значок в системной панели меняется. Так, например, если выполняется проверка скрипта, на фоне значка появляется небольшая пиктограмма со скриптом, а при проверке почтового сообщения – пиктограмма письма. По умолчанию анимация значка приложения используется. Если вы хотите отказаться от анимации, снимите флажок **Использовать анимацию значка при активности**. 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.

- *Уведомлять или нет о получении новостей от «Лаборатории Касперского».*

По умолчанию при получении новостей в системной панели появляется специальный значок, при нажатии на который открывается окно с текстом новости. Если вы хотите отключить уведомление, снимите флажок **Уведомлять о новостях с помощью значка в системной панели**.

- Показывать или нет индикатор защиты Антивируса Касперского при старте операционной системы.

По умолчанию такой индикатор появляется в правом верхнем углу экрана в момент запуска приложения. Он информирует вас о том, что защита вашего компьютера от любого рода угроз включена. Если вы не хотите использовать индикатор защиты, снимите флажок

Показывать значок поверх экрана приветствия Microsoft Windows.

Обратите внимание, что изменение параметров интерфейса Антивируса Касперского не сохраняется при восстановлении параметров работы по умолчанию или удалении приложения.

15.9. Использование дополнительных сервисов

Антивирус Касперского предлагает вам воспользоваться следующими дополнительными сервисами (см. рис. 72):

- запуск Антивируса Касперского при старте операционной системы (см. п. 15.11 на стр. 208);
- уведомление пользователя о возникновении некоторых событий в работе приложения (см. п. 15.9.1 на стр. 198);
- самозащита Антивируса Касперского от выключения, удаления или изменения модулей, а также защита доступа к приложению паролем (см. п. 15.9.2 на стр. 203);
- экспорт/импорт параметров работы Антивируса Касперского (см. п. 15.9.3 на стр. 204);
- восстановление параметров по умолчанию (см. п. 15.9.4 на стр. 205).

Чтобы перейти к настройке использования перечисленных сервисов,

откройте окно настройки приложения и выберите раздел **Сервис**.

В правой части вы можете определять, использовать дополнительные сервисы в работе приложения или нет.

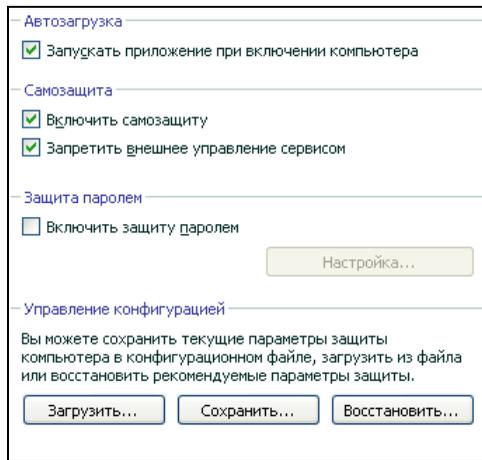


Рисунок 72. Настройка дополнительных сервисов

15.9.1. Уведомления о событиях Антивируса Касперского

В процессе работы Антивируса Касперского возникают различного рода события. Они могут быть информационного характера, а также нести важную информацию. Например, событие может уведомлять об успешно выполненном обновлении приложения, а может фиксировать ошибку в работе некоторого компонента, которую необходимо срочно устранить.

Для того чтобы быть в курсе событий в работе Антивируса Касперского, вы можете воспользоваться сервисом уведомлений.

Уведомления могут быть реализованы одним из следующих способов:

- Всплывающие сообщения над значком приложения в системной панели.
- Звуковое оповещение.
- Сообщения электронной почты.
- Запись информации в журнал событий.

Чтобы воспользоваться данным сервисом, вам нужно:

1. Установить флажок **Включить уведомления о событиях** в блоке **Уведомление о событиях** раздела **Вид** окна настройки приложения (см. рис. 71).

2. Определить типы событий Антивируса Касперского, о возникновении которых вы хотите быть уведомлены, и способ уведомлений (см. п. 15.9.1.1 на стр. 199).
3. Настроить параметры отправки уведомлений по электронной почте, если предполагается именно такой способ уведомлений (см. п. 15.9.1.2 на стр. 201).

15.9.1.1. Типы событий и способы 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 приложения или на уязвимости в защите вашего компьютера. Например, *базы приложения повреждены* или *истек срок действия ключа*.

Отказ функциональности – события, приводящие к неработоспособности приложения. Например, отсутствие ключа и баз приложения.

Важные события – события, на которые обязательно нужно обратить внимание, поскольку они отображают важные ситуации в работе приложения. Например, *защита отключена* или *компьютер давно не проверялся на присутствие вирусов*.

Информационные события – события справочного характера, как правило, не несущие важной информации. Например, *все опасные объекты вылечены*.

Чтобы указать, о каких событиях и каким образом вы должны быть уведомлены:

1. Откройте окно настройки приложения и выберите раздел **Вид** (см. рис. 71).
2. Установите флажок **Включить уведомление о событиях** в блоке **Уведомление о событиях** и перейдите к детальной настройке по кнопке **Дополнительно**.

В окне **Настройка уведомлений о событиях** (см. рис. 73) вы можете настроить следующие способы уведомлений о перечисленных выше событиях:

- *Всплывающее сообщение* над значком приложения в системной панели, содержащее информационное сообщение о возникшем событии.

Чтобы использовать данный тип уведомления, установите флажок в графе **Экран** напротив события, о котором вы хотите быть уведомлены.

- *Звуковое оповещение.*

Если вы хотите, чтобы данное уведомление сопровождалось звуковым сигналом, установите в графе **Звук** флажок напротив события.

- *Уведомление по электронной почте.*

Чтобы использовать данный тип уведомления, установите флажок в графе **E-mail** напротив события, о котором вы хотите быть уведомлены, и настройте параметры отправки уведомлений (см. п. 15.9.1.2 на стр. 201).

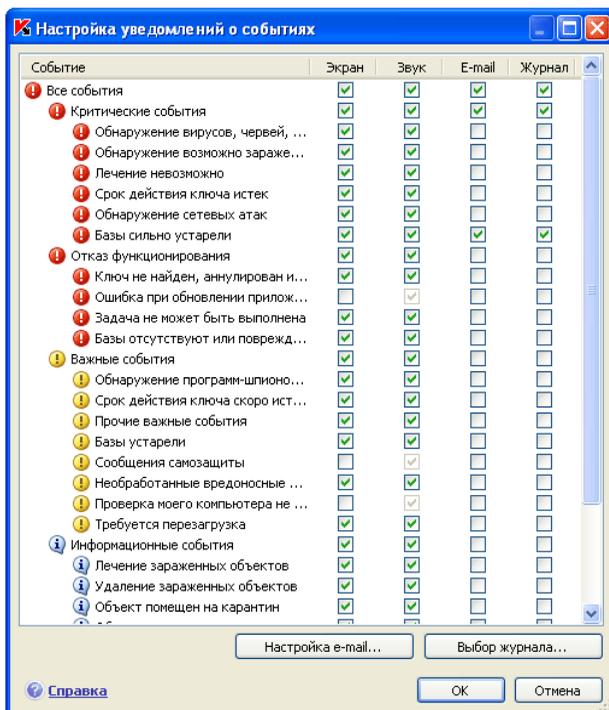


Рисунок 73. События в работе приложения и способы уведомлений о них

- *Запись информации в журнал событий.*

Чтобы фиксировать информацию о наступлении какого-либо события в журнале, установите напротив него флажок в графе **Журнал** и настройте параметры журнала событий (см. п. 15.9.1.3 на стр. 202).

15.9.1.2. Настройка отправки уведомлений по электронной почте

После того как вы выбрали события (см. п. 15.9.1.1 на стр. 199), уведомления о возникновении которых вы хотите получать по электронной почте, необходимо настроить отправку уведомлений. Для этого:

1. Откройте окно настройки приложения и выберите раздел **Вид** (см. рис. 71).
2. Нажмите на кнопку **Дополнительно** в блоке **Уведомление о событиях**.
3. В окне **Настройка уведомлений о событиях** (см. рис. 74) установите в графе **E-mail** флажок для событий, при наступлении которых требуется отправлять уведомление по электронной почте.
4. В окне (см. рис. 74), открываемом по кнопке **Настройка e-mail** задайте следующие параметры отправки уведомлений по почте:
 - Задайте параметры отправки уведомлений в блоке **Отправка уведомлений от имени**.
 - Укажите адрес электронной почты, на который будут отправляться уведомления в блоке **Получатель уведомлений**.
 - Задайте режим отправки уведомлений по электронной почте в блоке **Режим рассылки**. Чтобы приложение отправляла письмо по факту возникновения события, выберите  **При возникновении события**. Для уведомления о событиях за определенный промежуток времени сформируйте расписание отправки информационного письма, нажав на кнопку **Изменить**. По умолчанию предлагается ежедневное уведомление.

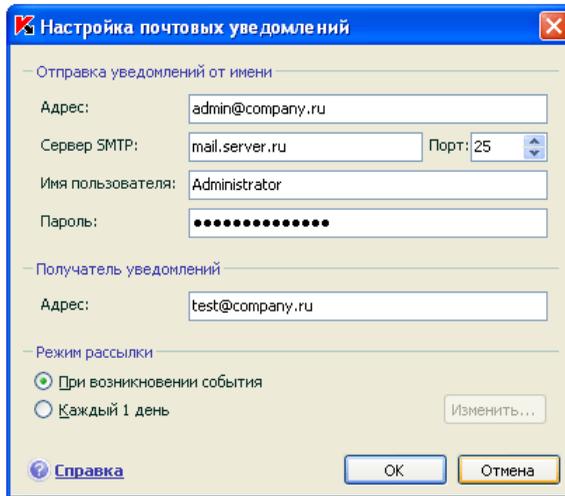


Рисунок 74. Настройка параметров уведомления по электронной почте

15.9.1.3. Настройка параметров журнала событий

Чтобы настроить параметры журнала событий:

1. Откройте окно настройки приложения и выберите раздел **Вид** (см. рис. 71).
2. Нажмите на кнопку **Дополнительно** в блоке **Уведомление о событиях**.

В окне **Настройка уведомлений о событиях** выберите для какого-либо события возможность записи информации в журнал и нажмите на кнопку **Выбор журнала**.

Антивирус Касперского предоставляет возможность записи информации о событиях, возникающих в работе приложения, в общий журнал событий Microsoft Windows (**Приложение**) 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**.

15.9.2. Самозащита приложения и ограничение доступа к ней

Антивирус Касперского является приложением, обеспечивающей безопасность компьютера от вредоносных программ, и в силу этого сама становится объектом интереса со стороны вредоносного программного обеспечения, пытающегося заблокировать работу приложения или даже удалить ее с компьютера.

Кроме того, персональный компьютер может использоваться несколькими людьми, в том числе с разным уровнем компьютерной грамотности. Открытый доступ к приложению, его параметрам может значительно снизить уровень безопасности компьютера в целом.

Чтобы обеспечить стабильность системы безопасности вашего компьютера, в приложение добавлены механизмы самозащиты, защиты от удаленного воздействия, а также защита доступа к приложению паролем.

Под управлением 64-разрядных операционных систем и Microsoft Windows Vista доступно только управление механизмом самозащиты приложения от изменения или удаления собственных файлов на диске, а также записей в системном реестре.

Чтобы включить использование механизмов самозащиты приложения:

1. Откройте окно настройки приложения и выберите раздел **Сервис** (см. рис. 72).
2. В блоке **Самозащита** выполните необходимую настройку:

Включить самозащиту. Если установлен этот флажок будет задействован механизм защиты приложения от изменения или удаления собственных файлов на диске, процессов в памяти, записей в системном реестре.

Запретить внешнее управление сервисом. При установленном флажке будет заблокирована любая попытка удаленного управления сервисами приложения.

При попытке выполнить какое-либо из перечисленных действий над значком приложения в системной панели будет открыто уведомление (если сервис уведомлений не отключен пользователем).

Чтобы защитить доступ к приложению с помощью пароля, установите флажок **Включить защиту паролем** в одноименном блоке и в окне, открываемом по кнопке **Настройка**, укажите пароль и область, на которую будет распространяться ограничение доступа (см. рис. 75). Вы можете заблокировать любые операции с приложением, за исключением работы с уве-

домлениями об обнаружении опасных объектов, или запретить выполнение одного из следующих действий:

- Изменить параметры работы приложения.
- Завершить работу Антивируса Касперского.
- Выключить защиту вашего компьютера или приостановить ее на некоторое время.

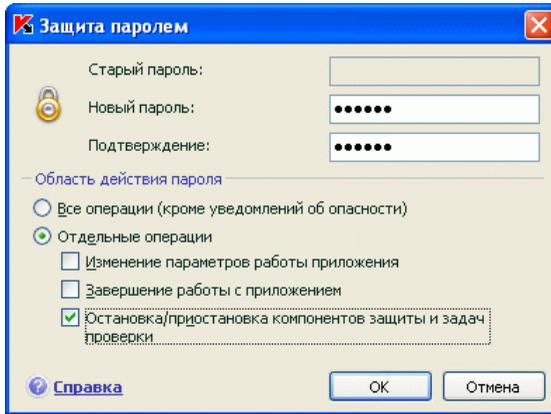


Рисунок 75. Настройка защиты приложения паролем

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.

Теперь при попытке любого пользователя на вашем компьютере выполнить выбранные вами действия приложение всегда будет запрашивать пароль.

15.9.3. Экспорт / импорт параметров работы Антивируса Касперского

Антивирус Касперского предоставляет вам возможность экспорта и импорта своих параметров.

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

Для того чтобы экспортировать текущие параметры работы приложения,

1. Откройте окно настройки приложения и выберите раздел **Сервис** (см. рис. 72).
2. Нажмите на кнопку **Сохранить** в блоке **Управление конфигурацией**.
3. Введите название конфигурационного файла и укажите место его сохранения.

Для импорта параметров работы из конфигурационного файла

1. Откройте окно настройки приложения и выберите раздел **Сервис**.
2. Нажмите на кнопку **Загрузить** и выберите файл, из которого вы хотите импортировать параметры Антивируса Касперского.

15.9.4. Восстановление параметров по умолчанию

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

Чтобы восстановить параметры защиты,

1. Откройте окно настройки приложения и выберите раздел **Сервис** (см. рис. 72).
2. Нажмите на кнопку **Восстановить** в блоке **Управление конфигурацией**.

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

В списке представлены компоненты приложения, параметры которых были изменены пользователем. Если для какого-либо из компонентов в процессе работы были сформированы уникальные параметры, они также будут представлены в списке.

Таковыми уникальными параметрами являются сформированные правила исключений защиты для компонентов приложения, списки доверенных интернет-адресов, используемых Веб-Антивирусом, а также правила для приложений Проактивной защиты.

Данные списки формируются в процессе работы с приложением, исходя из индивидуальных задач и требований безопасности, и их формирование зачастую занимает много времени. Поэтому мы рекомендуем сохранять их при восстановлении первоначальных параметров работы приложения.

По умолчанию все уникальные параметры, представленные в списке, подлежат сохранению (флажки напротив них сняты). Если сохранение какого-либо из параметров не требуется, установите напротив него флажок.

По завершении настройки нажмите на кнопку **Далее**. Будет запущен мастер первоначальной настройки приложения (см. п. 3.2 на стр. 35). Следуйте его указаниям.

По завершении работы мастера для всех компонентов защиты будет установлен **Рекомендуемый** уровень безопасности с учетом тех параметров, которые вы решили сохранить при восстановлении. Кроме того, будут использоваться параметры, которые вы настроили в ходе работы мастера.

15.10. Техническая поддержка пользователей

Информация о технической поддержке, предоставляемой «Лабораторией Касперского» пользователям, представлена в разделе **Поддержка** (см. рис. 76) главного окна приложения.

В верхней части вы можете просмотреть общую информацию о приложении: версия приложения, дата выпуска используемых приложением баз, а также краткие данные об установленной на вашем компьютере операционной системе.

Если при использовании Антивируса Касперского возникли проблемы, прежде всего убедитесь, не описан ли метод решения вашей проблемы в данной справочной системе или в Базе знаний на веб-сайте Службы технической поддержки «Лаборатории Касперского». 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. Для перехода к Базе знаний воспользуйтесь ссылкой [Техническая поддержка онлайн](#).

Еще один ресурс, где вы можете получить информацию по работе с приложением, – это Форум пользователей продуктов «Лаборатории Касперского». Данный ресурс также является отдельным разделом веб-сайта Службы технической поддержки и содержит вопросы, отзывы и пожелания пользователей приложения. Вы можете ознакомиться с основными темами форума, оставить отзыв о приложении или отыскать ответ на свой вопрос. Чтобы перейти к этому ресурсу, воспользуйтесь ссылкой [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».

Обратите внимание, что для получения технической поддержки вы должны быть зарегистрированным пользователем коммерческой версии Антивируса Касперского. Поддержка пользователей пробных версий приложения не осуществляется.

Регистрация пользователя выполняется через мастер активации приложения (см. п. 3.2.2 на стр. 36), в случае если вы активируете приложение с помощью кода активации. В данном случае по окончании регистрации вам будет присвоен номер клиента, который можно посмотреть в разделе **Поддержка** (см. рис. 76) главного окна. Номер клиента - это персональный идентификационный номер пользователя, который является обязательным условием для получения технической поддержки по телефону или через веб-форму.

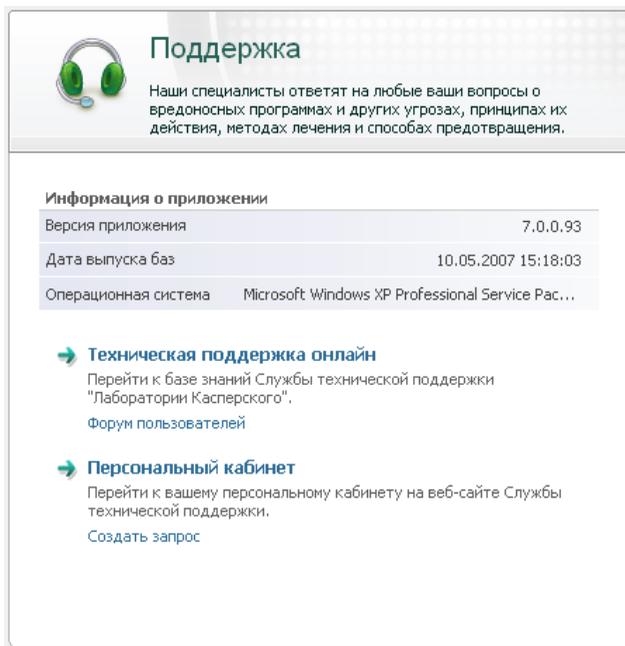
Если вы активируете приложение с помощью файла ключа, пройдите процедуру регистрации непосредственно на веб-сайте Службы технической поддержки.

Новый сервис – **Персональный кабинет** – обеспечивает доступ пользователя к личному разделу на веб-сайте Службы технической поддержки. В Персональном кабинете вы можете:

- отправлять запрос в Службу поддержки без предварительного ввода регистрационной информации;
- переписываться со Службой поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени;
- просматривать полную историю ваших обращений в Службу поддержки;
- получать резервную копию файла ключа.

Для обращения в Службу технической поддержки через веб-форму воспользуйтесь ссылкой [Создать запрос](#). На открывшейся веб-странице Службы технической поддержки войдите в свой Персональный кабинет и заполните форму запроса.

Для решения срочных проблем позвоните по указанным в справке контактными телефонам (см. п. С.2 на стр. 250). Поддержка пользователей по телефону осуществляется в круглосуточном режиме на русском, английском, французском, немецком и испанском языках.



Поддержка

Наши специалисты ответят на любые ваши вопросы о вредоносных программах и других угрозах, принципах их действия, методах лечения и способах предотвращения.

Информация о приложении

Версия приложения	7.0.0.93
Дата выпуска баз	10.05.2007 15:18:03
Операционная система	Microsoft Windows XP Professional Service Pac...

- **Техническая поддержка онлайн**
Перейти к базе знаний Службы технической поддержки "Лаборатории Касперского".
[Форум пользователей](#)
- **Персональный кабинет**
Перейти к вашему персональному кабинету на веб-сайте Службы технической поддержки.
[Создать запрос](#)

Рисунок 76. Информация о технической поддержке

15.11. Завершение работы с приложением

Если по какой-либо причине вам требуется полностью завершить работу Антивируса Касперского, выберите пункт **Выход** контекстного меню (см. п. 4.2 на стр. 45) приложения. В результате приложение будет выгружено из оперативной памяти, что подразумевает, что ваш компьютер на данный период работает в незащищенном режиме.

Если в момент завершения работы на компьютере были установлены сетевые соединения, контролируемые приложением, на экран будет выведено уведомление о разрыве этих соединений. Это необходимо для корректного завершения приложения. Разрыв происходит автоматически по истечении 10 секунд либо при нажатии на кнопку **Да**. Большинство прерванных соединений восстанавливается через некоторое время.

Обратите внимание, что если во время разрыва соединения вы скачиваете файл без использования менеджера загрузки, передача данных будет прервана. Для получения файла вам потребуется повторно инициировать его загрузку.

Вы можете отменить разрыв соединений, для этого в окне уведомления нажмите на кнопку **Нет**. При этом приложение продолжит свою работу.

Если вы завершили работу приложения, включить защиту компьютера снова вы можете, загрузив приложение Антивирус Касперского из меню **Пуск** → **Программы** → **Антивирус Касперского 7.0** → **Антивирус Касперского 7.0**.

Также защита может быть запущена автоматически после перезагрузки операционной системы. Чтобы включить этот режим в окне настройки приложения выберите раздел **Сервис** (см. рис. 72) и установите флажок **Запускать приложение при включении компьютера** в блоке **Автозагрузка**.

ГЛАВА 16. РАБОТА С ПРИЛОЖЕНИЕМ ИЗ КОМАНДНОЙ СТРОКИ

Вы можете работать с Антивирусом Касперского посредством командной строки. При этом предусмотрена возможность выполнения следующих операций:

- запуск, остановка, приостановка и возобновление работы компонентов приложения;
- запуск, остановка, приостановка и возобновления выполнения задач проверки на вирусы;
- получение информации о текущем статусе компонентов и задач и их статистики;
- проверка выбранных объектов;
- обновление баз и модулей приложения;
- вызов справки по синтаксису командной строки;
- вызов справки по синтаксису команды.

Синтаксис командной строки:

```
avr.com <команда> [параметры]
```

Обращение к приложению через командную строку должно осуществляться из каталога установки продукта либо с указанием полного пути к avr.com.

В качестве **<команд>** используются:

ACTIVATE	активация приложения через интернет с помощью кода активации
ADDKEY	активация приложения с помощью файла ключа (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
START	запуск компонента или задачи

PAUSE	приостановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
RESUME	возобновление работы компонента или задачи
STOP	остановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
STATUS	вывод на экран текущего статуса компонента или задачи
STATISTICS	вывод на экран статистики по работе компонента или задачи
HELP	помощь по синтаксису команды, вывод списка команд
SCAN	проверка объектов на присутствие вирусов
UPDATE	запуск обновления приложения
ROLLBACK	откат последнего произведенного обновления приложения (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
EXIT	завершение работы с приложением (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
IMPORT	импорт параметров защиты приложения (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
EXPORT	экспорт параметров защиты приложения

Каждой команде соответствует собственный набор параметров, специфичный для конкретного компонента Антивируса Касперского.

16.1. Активация приложения

Активацию приложения возможно произвести двумя способами:

- через интернет с помощью кода активации (команда ACTIVATE);
- с помощью файла ключа (команда ADDKEY).

Синтаксис команды:

```
ACTIVATE <код_активации>
ADDKEY <имя_файла> /password=<ваш_пароль>
```

Описание параметров:

<код_активации>	код активации приложения, предоставленный при покупке.
<имя_файла>	имя файла ключа к приложению с расширением *.key.
<ваш_пароль>	пароль к Антивирусу Касперского, заданный в интерфейсе приложения.
Обратите внимание, что без ввода пароля команда ADDKEY выполняться не будет.	

Пример:

```
avp.com ACTIVATE 00000000-0000-0000-0000-000000000000
avp.com ADDKEY 00000000.key /password=<ваш_пароль>
```

16.2. Управление компонентами приложения и задачами

Синтаксис команды:

```
avp.com <команда> <профайл|имя_задачи>
[/R[A]:<файл_отчета>]
avp.com STOP|PAUSE <профайл|имя_задачи>
/password=<ваш_пароль> [/R[A]:<файл_отчета>]
```

Описание параметров:

<команда>	Управление компонентами и задачами Антивируса Касперского из командной строки выпол-
------------------------	--

	<p>няется с помощью следующего набора команд:</p> <p>START – запуск компонента постоянной защиты или задачи.</p> <p>STOP – остановка работы компонента постоянной защиты или задачи.</p> <p>PAUSE – приостановка работы компонента постоянной защиты или задачи.</p> <p>RESUME – возобновление работы компонента постоянной защиты или задачи.</p> <p>STATUS – вывод на экран текущего статуса компонента постоянной защиты или задачи.</p> <p>STATISTICS – вывод на экран статистики по работе компонента постоянной защиты или задачи.</p> <p>Обратите внимание, что без ввода пароля команды PAUSE и STOP выполняться не будут.</p>
<профайл имя_задачи>	<p>В качестве значений для параметра <профайл> вы можете указать любой из компонентов постоянной защиты приложения, а также модули, входящие в состав компонентов, сформированные задачи проверки по требованию или обновления (используемые приложением стандартные значения приводятся в таблице ниже).</p> <p>В качестве значений для параметра <имя_задачи> может быть указано имя любой сформированной пользователем задачи проверки по требованию либо обновления.</p>
<ваш_пароль>	<p>пароль к Антивирусу Касперского, заданный в интерфейсе приложения.</p>
/R[A]:<файл_отчета>	<p>R:<файл_отчета> – фиксировать в отчете только важные события.</p> <p>/RA:<файл_отчета> – записывать в отчет все события.</p> <p>Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на эк-</p>

	ран, отображаются все события.
--	--------------------------------

В качестве параметра <профайл> указывается одно из следующих значений:

RTP	<p>все компоненты защиты</p> <p>Команда <code>avp.com START RTP</code> запускает все компоненты постоянной защиты, если защита была полностью отключена (см. п. 6.1.2 на стр. 61) либо приостановлена на время (см. п. 6.1.1 на стр. 60). Также данная команда запускает любой из компонентов постоянной защиты, работа которого приостановлена из графического интерфейса приложения либо командой <code>PAUSE</code> командной строки.</p> <p>В случае если компонент был выключен из графического интерфейса приложения либо командой <code>STOP</code> командной строки, он не будет запущен командой <code>avp.com START RTP</code>. Для этого необходимо выполнить команду <code>avp.com START <профайл></code>, где в качестве <профайл> используется значение для конкретного компонента защиты, например, <code>avp.com START FM</code>.</p>
FM	Файловый Антивирус
EM	Почтовый Антивирус
WM	<p>Веб-Антивирус</p> <p>Значения для подкомпонентов Веб-Антивируса:</p> <p><code>httpscan</code> – проверка http-трафика;</p> <p><code>sc</code> – проверка скриптов.</p>
BM	<p>Проактивная защита</p> <p>Значения для подкомпонентов Проактивной защиты:</p> <p><code>pdm</code> – анализ активности приложений.</p>
UPDATER	Обновление

Rollback	Откат последнего обновления
SCAN_OBJECTS	задача «Поиск вирусов»
SCAN_MY_COMPUTER	задача «Мой Компьютер»
SCAN_CRITICAL_AREAS	задача «Критические области»
SCAN_STARTUP	задача «Объекты автозапуска»
SCAN_QUARANTINE	задача проверки объектов карантина
SCAN_ROOTKITS	задача поиска руткитов (rootkit)
Компоненты и задачи, запущенные из командной строки, выполняются с параметрами, установленными в интерфейсе продукта.	

Примеры:

Для того чтобы включить Файловый Антивирус, в командной строке введите:

```
avp.com START FM
```

Для просмотра текущего статуса Проактивной защиты вашего компьютера в командной строке введите:

```
avp.com STATUS BM
```

Для остановки задачи проверка Моего Компьютера в командной строке введите:

```
avp.com STOP SCAN_MY_COMPUTER /password=<ваш_пароль>
```

16.3. Антивирусная проверка объектов

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>] [<конфигурационный файл>]
[<параметры отчета>] [<дополнительные параметры>]
```

Для проверки объектов вы также можете воспользоваться сформированными в Антивирусе Касперского задачами, запустив нужную из командной строки (см. п. 16.1 на стр. 212). При этом задача будет выполнена с параметрами, установленными в интерфейсе продукта.

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>	<p>Список путей к файлам и/или каталогам для проверки. Допускается ввод абсолютного или относительного пути. Разделительный символ для элементов списка – пробел.</p> <p>Замечания:</p> <ul style="list-style-type: none"> • если имя объекта содержит пробел, оно должно быть заключено в кавычки; • если указан конкретный каталог, проверяются все файлы, содержащиеся в нем.
/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.
/ALL	полная проверка компьютера.

/@:<filelist.lst>	<p>путь к файлу со списком объектов и каталогов, включаемых в проверку. Файл должен иметь текстовый формат; каждый объект проверки необходимо указывать с новой строки.</p> <p>Допускается ввод абсолютного или относительного пути к файлу. Путь указывается в кавычках, если в нем содержится символ «пробел».</p>
<p><действие> - параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению /i8.</p>	
/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.
<p><типы файлов> - 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 содержанию.
/fa	проверять все файлы.
<p><исключения> - параметр определяет объекты, исключаемые из проверки. Параметр может включать несколько значений из представленного списка, разделенных пробелом.</p>	
-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 МБ) превышает значение, заданное параметром <size>.
<p><конфигурационный файл> - определяет путь к конфигурационному файлу, содержащему параметры работы приложения при проверке.</p> <p>Конфигурационный файл представляет собой файл текстового формата, содержащий набор параметров командной строки для антивирусной проверки.</p> <p>Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе Антивируса Касперского.</p>	
/c:<имя_файла>	использовать значения параметров, заданные в конфигурационном файле <имя_файла>.

<p><параметры отчета> - параметр определяет формат отчета о результатах проверки.</p> <p>Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.</p>	
/R:<файл_отчета>	записывать в указанный файл отчета только важные события.
/RA:<файл_отчета>	записывать в указанный файл отчета все события.
<p><дополнительные параметры> – параметр, определяющий использование технологий антивирусной проверки.</p>	
/iChecker=<on off>	включить/отключить использование технологии iChecker.
/iSwift=<on off>	включить/отключить использование технологии iSwift.

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"
```

Приостановить проверку выбранных объектов, запустить полную проверку компьютера, по окончании которой продолжить поиск вирусов среди выбранных объектов:

```
avp.com PAUSE SCAN_OBJECTS /password=<ваш_пароль>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*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 /@:object2scan.txt
/C:scan_setting.txt /RA:scan.log
```

Пример конфигурационного файла:

```

/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log

```

16.4. Обновление приложения

Команда для обновления баз и модулей Антивируса Касперского имеет следующий синтаксис:

```

avp.com UPDATE [<источник_обновлений>]
[/R[A]:<файл_отчета>] [/C:<имя_файла>] [/APP=<on|off>]

```

Описание параметров:

<источник_обновлений>	<p>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 приложения.</p>
/R[A]:<файл_отчета>	<p>/R:<файл_отчета> - фиксировать в отчете только важные события.</p> <p>/RA:<файл_отчета> - записывать в отчет все события.</p> <p>Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.</p>

<code>/C:<имя_файла></code>	<p>путь к конфигурационному файлу, содержащему параметры работы приложения при обновлении.</p> <p>Конфигурационный файл представляет собой файл текстового формата, содержащий набор параметров командной строки для обновления приложения.</p> <p>Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения параметров, установленные в интерфейсе Антивируса Касперского.</p>
<code>/APP=<on off></code>	включить/ отключить обновление модулей приложения.

Примеры:

Обновить базы Антивируса Касперского, 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
```

Пример конфигурационного файла:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt  
/app=on
```

16.5. Откат последнего обновления приложения

Синтаксис команды:

```
ROLLBACK [/R[A]:<файл_отчета>] [/password=<ваш_пароль>]
```

/R[A]:<файл_отчета>	<p>/R:<файл_отчета> - фиксировать в отчете только важные события.</p> <p>/RA:<файл_отчета> - записывать в отчет все события.</p> <p>Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.</p>
<ваш_пароль>	пароль к Антивирусу Касперского, заданный в интерфейсе приложения.

Обратите внимание, что без ввода пароля данная команда выполняться не будет.

Пример:

```
avp.com ROLLBACK /RA:rollback.txt /password=<ваш_пароль>
```

16.6. Экспорт параметров защиты

Синтаксис команды:

```
avp.com EXPORT <профайл> <имя_файла>
```

Описание параметров:

<имя_файла>	<p>путь к файлу, в который экспортируются параметры Антивируса Касперского. Может быть указан абсолютный или относительный путь.</p> <p>Конфигурационный файл сохраняется в бинарном формате (<i>dat</i>), если не указан иной формат либо формат не задан, и далее может использоваться для переноса параметров приложения на другие компьютеры. Кроме того, вы можете сохранить конфигурационный файл в текстовом формате, для этого в имени файла укажите расширение <i>txt</i>. Обратите внимание, что импорт параметров защиты из текстового файла не поддерживается, данный файл может использоваться только для просмотра основных параметров работы приложения.</p>
-------------	---

<профайл>	компонент или задача, для которых выполняется экспорт параметров. В качестве значения параметра <профайл> может быть использовано любое значение, указанное в п. 16.2 на стр. 212.
------------------------	--

Пример:

```
avp.com EXPORT c:\settings.dat
```

16.7. Импорт параметров защиты

Синтаксис команды:

```
avp.com IMPORT <имя_файла> [/password=<ваш_пароль>]
```

<имя_файла>	путь к файлу, из которого импортируются параметры Антивируса Касперского. Может быть указан абсолютный или относительный путь. Импорт параметров защиты возможен только из файла в бинарном формате.
<ваш_пароль>	пароль к Антивирусу Касперского, заданный в интерфейсе приложения.
Обратите внимание, что без ввода пароля данная команда выполняться не будет.	

Пример:

```
avp.com IMPORT c:\settings.dat /password=<ваш_пароль>
```

16.8. Запуск приложения

Синтаксис команды:

```
avp.com
```

16.9. Остановка приложения

Синтаксис команды:

```
EXIT /password=<ваш_пароль>
```

<ваш_пароль>	пароль к Антивирусу Касперского, заданный в интерфейсе приложения.
Обратите внимание, что без ввода пароля данная команда выполняться не будет.	

16.10. Получение файла трассировки

Создание файла трассировки может потребоваться при наличии проблем в работе приложения 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>	<p>Для данного параметра допустимо указывать числовое значение в диапазоне от 0 (минимальный уровень, только критические сообщения) до 700 (максимальный уровень, все сообщения).</p> <p>При обращении в Службу технической поддержки специалист должен указать необходимый уровень трассировки. Если он не был указан, то рекомендуется устанавливать уровень 500.</p>

Внимание! Рекомендуется включать создание файлов трассировки только для диагностики конкретной проблемы. Постоянное включение трассировки может привести к потере производительности работы компьютера и переполнению жесткого диска.

Примеры:

Отключить создание файлов трассировки:

```
avp.com TRACE file off
```

Создать файл трассировки для отправки в Службу технической поддержки с максимальным уровнем трассировки равным 500:

```
avp.com TRACE file on 500
```

16.11. 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>
```

16.12. Коды возврата командной строки

В данном разделе приведено описание кодов 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 поиска вирусов	
101	Все опасные объекты обработаны
102	Обнаружены опасные объекты

ГЛАВА 17. ИЗМЕНЕНИЕ, ВОССТАНОВЛЕНИЕ ИЛИ УДАЛЕНИЕ ПРИЛОЖЕНИЯ

Удалить приложение можно следующими способами:

- с помощью мастера установки приложения (см. п. 17.1 на стр. 226);
- из командной строки (см. п. 17.2 на стр. 228).

17.1. Изменение, восстановление и удаление приложения с помощью мастера установки

Восстановление приложения полезно проводить в том случае, если вы обнаружили какие-либо ошибки в ее работе вследствие некорректной настройки или повреждения его файлов.

Изменение компонентного состава позволяет вам доустановить недостающие компоненты Антивируса Касперского или удалить те их них, которые мешают вам в работе или не требуются.

Для того чтобы перейти к восстановлению исходного состояния приложения, установке компонентов Антивируса Касперского, которые не были установлены изначально, или удалению приложения,

1. Выгрузите приложение из оперативной памяти. Для этого щелкните правой клавишей мыши на значке приложения в системной панели и в открывшемся контекстном меню выберите пункт **Выход**.
2. Вставьте CD-диск с дистрибутивом приложения в CD/DVD-ROM-устройство, если установка приложения производилась с него. В случае установки Антивируса Касперского из другого источника (папка общего доступа, папка на жестком диске и т.д.) убедитесь, что дистрибутив приложения присутствует там и у вас есть к нему доступ.
3. Выберите **Пуск → Программы → Антивирус Касперского 7.0 → Изменение, восстановление или удаление**.

В результате будет запущена программа установки, которая выполнена в виде мастера. Рассмотрим подробнее шаги по восстановлению, изменению компонентного состава приложения и его удалению.

Шаг 1. Выбор операции

Сначала вам нужно определить, какую именно операцию вы хотите выполнить над приложением: вам предлагается изменить компонентный состав приложения, восстановить исходное состояние установленных компонентов или удалить какие-либо компоненты или приложение 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 приложения (см. Шаг 6 на стр. 33), где вы можете указать, какие компоненты вы хотите установить, а также выбрать те, которые хотите удалить.

Восстановление приложения 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 удалении приложения вы можете выбрать, какие данные, сформированные и используемые в работе приложения, вы хотите сохранить на вашем компьютере. Чтобы удалить все данные Антивируса Касперского, выберите вариант  **Удалить приложение полностью**. Для сохранения данных вам нужно выбрать вариант  **Сохранить объекты приложения и указать, какие именно объекты не нужно удалять**:

- *Информация об активации* – файл ключа приложения.
- *Базы приложения* – 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 баз приложения.
- *Параметры защиты* – значения параметров работы всех компонентов приложения.

- *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.

Внимание!

Если между удалением одной версии Антивируса Касперского и установкой другой достаточно продолжительный промежуток времени, не рекомендуем вам использовать базу *iSwift*, сохраненную с предыдущей установки приложения. 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 2. Завершение операции восстановления, изменения или удаления приложения

Процесс восстановления, изменения или удаления будет отображаться на экране, после чего вы будете уведомлены о ее 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. Для того чтобы перезагрузить компьютер позже вручную, нажмите на кнопку **Нет**.

17.2. Удаление приложения из командной строки

Чтобы удалить Антивирус Касперского 7.0 из командной строки, наберите:

```
msiexec /x <имя_пакета>
```

Будет запущен мастер установки, с помощью которого вы сможете провести процедуру удаления приложения (см. п. Глава 17 на стр. 226).

Также для удаления вы можете воспользоваться описанными ниже командами.

Для того чтобы удалить приложение в скрытом режиме без перезагрузки компьютера (перезагрузку следует произвести вручную после удаления), наберите:

```
msiexec /x <имя_пакета> /qn
```

Для того чтобы удалить приложение в скрытом режиме с последующей перезагрузкой компьютера, наберите:

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

ГЛАВА 18. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

В данной главе мы осветим наиболее распространенные вопросы пользователей по установке, настройке и работе приложения и постараемся ответить на них наиболее подробно.

Вопрос: *возможно ли использование Антивируса Касперского 7.0 с антивирусными продуктами других производителей?*

Во избежание конфликтов мы рекомендуем удалять антивирусные продукты сторонних производителей до установки Антивируса Касперского.

Вопрос: *Антивирус Касперского не проверяет файл повторно. Почему?*

Действительно Антивирус Касперского не проверяет повторно файлы, которые не изменились с момента последней проверки.

Это возможно благодаря применению новых технологий iChecker™ и iSwift™. Для реализации технологии используется база контрольных сумм объектов и хранение контрольных сумм файлов в дополнительных потоках NTFS.

Вопрос: *для чего требуется активация приложения? Может ли Антивирус Касперского работать без файла ключа?*

Антивирус Касперского может работать без ключа, однако сервис обновления приложения и помощь Службы технической поддержки не будут доступны.

Если вы еще не решились на приобретение Антивируса Касперского, мы можем предоставить вам пробный ключ, который будет работать в течение двух недель или месяца. По истечении данного срока ключ будет заблокирован.

Вопрос: *после установки Антивируса Касперского операционная система начала вести себя нестандартным образом («падение в синий экран», постоянная перезагрузка компьютера и т.п.). Что делать?*

Такая ситуация редка, но возможна при конфликте Антивируса Касперского и программного обеспечения, установленного на вашем компьютере.

Для восстановления работоспособности операционной системы выполните следующие действия:

1. В самом начале загрузки компьютера нажимайте на клавишу **F8** до тех пор, пока не отобразится меню выбора вариантов загрузки операционной системы.
2. Выберите пункт **Безопасный режим** и загрузите операционную систему.
3. Запустите Антивирус Касперского.
4. Откройте окно настройки приложения и выберите раздел **Сервис**.
5. Снимите флажок **Запускать приложение при включении компьютера** и нажмите на кнопку **ОК**.
6. Перезагрузите операционную систему в обычном режиме.

Отправьте запрос в Службу технической поддержки «Лаборатории Касперского». Для этого откройте главное окно приложения, выберите раздел **Поддержка** и воспользуйтесь ссылкой [Создать запрос](#). Как можно подробнее опишите проблему и условия, в которых она возникает.

К запросу обязательно приложите файл полного дампа памяти операционной системы Microsoft Windows. Для его создания выполните следующие действия:

1. Нажмите правой клавишей мыши на значок **Мой Компьютер** и в открывшемся контекстном меню выберите пункт **Свойства**.
2. В окне **Свойства системы** выберите закладку **Дополнительно** и в разделе **Загрузка и восстановление** нажмите на кнопку **Параметры**.
3. В окне **Загрузка и восстановление** в разделе **Запись отладочной информации** из раскрывающегося списка выберите значение **Полный дамп памяти**.

По умолчанию файл дампа сохраняется в системный каталог под именем *memory.dmp*. Вы можете изменить каталог хранения дампа, для этого измените имя каталога в соответствующем поле.

4. Воспроизведите проблему, связанную с работой Антивируса Касперского.
5. Убедитесь, что файл полного дампа памяти успешно сохранен.

ПРИЛОЖЕНИЕ А.

СПРАВОЧНАЯ ИНФОРМАЦИЯ

В данном приложении содержится справочная информация по форматам проверяемых файлов и разрешенным маскам, используемым при настройке Антивируса Касперского.

А.1. Список объектов, проверяемых по расширению

Если в качестве объектов проверки Файлового Антивируса вы выбрали  **Проверять программы и документы (по расширению)**, то будут детально анализироваться на присутствие вирусов файлы с приведенными ниже расширениями. Такие же файлы проверяются Почтовым Антивирусом, если вы включили фильтрацию присоединенных к почтовому сообщению объектов:

com – исполняемый файл программы.

exe – исполняемый файл, самораспаковывающийся архив.

sys – системный драйвер.

prg – текст программы dBase, Clipper или Microsoft Visual FoxPro, программа пакета WAVmaker.

bin – бинарный файл.

bat – файл пакетного задания.

cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2.

dpl – упакованная библиотека Borland Delphi.

dll – библиотека динамической загрузки.

scr – файл-заставка экрана Microsoft Windows.

cpl – модуль панели управления (control panel) в Microsoft Windows.

ocx – объект Microsoft OLE (Object Linking and Embedding).

tsp – программа, работающая в режиме разделения времени.

drv – драйвер некоторого устройства.

vxd – драйвер виртуального устройства Microsoft Windows.

pif – файл с информацией о программе.

lnk – файл-ссылка в Microsoft Windows.
reg – файл регистрации ключей системного реестра Microsoft Windows.
ini – файл инициализации.
cla – класс Java.
vbs – скрипт Visual Basic.
vbe – видео-расширение BIOS.
js, jse – исходный текст JavaScript.
htm – гипертекстовый документ.
htt – гипертекстовая заготовка Microsoft Windows.
hta – гипертекстовая программа для Microsoft Internet Explorer.
asp – скрипт Active Server Pages.
chm – скомпилированный HTML-файл.
pht – HTML-файл со встроенными скриптами PHP.
php – скрипт, встраиваемый в HTML-файлы.
wsh – файл Microsoft Windows Script Host.
wsf – скрипт Microsoft Windows.
the – файл заставки для рабочего стола Microsoft Windows 95
hlp – файл справки формата Win Help.
eml – почтовое сообщение Microsoft Outlook Express.
nws – новое почтовое сообщение Microsoft Outlook Express.
msg – почтовое сообщение Microsoft Mail.
plg – почтовое сообщение.
mbx – расширение для сохраненного письма Microsoft Office Outlook.
doc – документ Microsoft Office Word.
dot – шаблон документов Microsoft Office Word.
fpm – программа баз данных, стартовый файл Microsoft Visual FoxPro.
rtf – документ в формате Rich Text Format.
shs – фрагмент Shell Scrap Object Handler.
dwg – база данных чертежей AutoCAD.
msi – пакет Microsoft Windows Installer.
otm – VBA-проект для Microsoft Office Outlook.
pdf – документ Adobe Acrobat.
swf – объект пакета Shockwave Flash.
jpg, jpeg, png – файл графического формата хранения сжатых изображений.

emf – файл формата Enhanced Metafile. Следующее поколение мета-файла операционной системы Microsoft Windows. Файлы EMF не поддерживаются 16-разрядной Microsoft Windows.

ico – файл значка объекта.

ov? – исполняемые файлы MS DOC.

*xl** – документы и файлы Microsoft Office Excel, такие как: *x/a* – расширение Microsoft Office Excel, *x/c* – диаграмма, *x/t* – шаблон документов и т.д.

*pp** – документы и файлы Microsoft Office PowerPoint, такие как: *pps* – слайд Microsoft Office PowerPoint, *ppt* – презентация и т.д.

*md** – документы и файлы Microsoft Office Access, такие как: *mda* – рабочая группа Microsoft Office Access, *mdb* – база данных и т.д.

Помните, что фактический формат файла может не совпадать с форматом, указанным в расширении файла.

А.2. 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 один символ
 - **C:\dir\test** – только файл *C:\dir\test*

Для того чтобы не проверялись файлы во всех вложенных папках указанного каталога, при создании маски установите флажок



Включая вложенные папки.

3. Маски с относительными путями 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 каталогах *dir*, где вместо ? может использоваться любой один символ

Для того чтобы не проверялись файлы во всех вложенных папках указанного каталога, при создании маски установите флажок

Включая вложенные папки.

Совет.

Использовать маски исключения *.* или * допустимо только при указании типа исключаемой угрозы согласно Вирусной энциклопедии. В этом случае указанная угроза не будет обнаруживаться во всех объектах. Использование данных масок без указания типа угрозы равносильно отключению защиты.

Также не рекомендуется в качестве исключения выбирать виртуальный диск, сформированный на основе каталога файловой системы посредством команды *subst*. Это не имеет смысла, поскольку во время проверки приложение воспринимает этот виртуальный диск как каталог, следовательно, проверяет его.

А.3. Разрешенные маски исключений по классификации Вирусной энциклопедии

При добавлении в качестве исключения угрозы с определенным статусом по классификации Вирусной энциклопедии вы можете указать:

- полное имя угрозы, как оно представлено в вирусной энциклопедии на сайте www.viruslist.ru (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.

ПРИЛОЖЕНИЕ В. ООО «КРИПТОЭКС»

Для формирования и проверки электронной цифровой подписи в Антивирусе Касперского используется программная библиотека защиты информации (ПБЗИ) «Крипто-Си», разработанная ООО «КриптоЭкс».

ООО «КриптоЭкс» имеет лицензии ФАПСИ (ФСБ) на разработку, производство и распространение шифровальных средств комплексов, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну.

ПБЗИ «Крипто-Си» предназначена для использования в системах комплексной защиты конфиденциальной информации по классу КС1 и имеет сертификат соответствия ФСБ № СФ/114-0901 от 01 июля 2006 года.

Модули библиотеки реализуют шифрование и расшифровку блока данных фиксированной размерности и (или) потока данных в соответствии с криптографическим алгоритмом (ГОСТ 28147-89), генерацию и проверку электронной цифровой подписи в соответствии с алгоритмами (ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001), хэш-функцию (ГОСТ Р 34.11-94), генерацию ключевой информации с использованием программного датчика псевдослучайных чисел. Реализована также схема распределения ключевой информации и выработка имитовекторов (ГОСТ 28147-89).

Модули библиотеки реализованы на языке программирования «Си» (в соответствии со стандартом ANSI «С») и могут быть интегрированы в приложения в виде статически и динамически подгружаемого кода и поддерживают возможность исполнения на платформах x86, x86-64, Ultra SPARC II и совместимых с ними.

Модули библиотеки переносимы под операционные среды: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris для Ultra SPARC II).

Веб-сайт ООО «КриптоЭкс»: <http://www.cryptoex.ru>

E-mail: info@cryptoex.ru

ПРИЛОЖЕНИЕ С. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

ЗАО «Лаборатория Касперского» была основана в 1997 г. 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 четырехсот пятидесяти 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. Основным продуктом 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 западные разработчики используют в своих продуктах программное ядро Антивируса Касперского[®], например, такие как: Nokia ICG (США), F-Secure (Финляндия), 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 круглосуточной технической поддержкой на нескольких языках.

С.1. Другие разработки «Лаборатории Касперского»

Новостной Агент «Лаборатории Касперского»

Программа Новостной Агент предназначена для оперативной доставки новостей «Лаборатории Касперского», оповещения о «вирусной погоде» и появлении свежих новостей. С заданной периодичностью программа считывает с новостного сервера «Лаборатории Касперского» список доступных новостных каналов и содержащуюся в них информацию.

Новостной Агент также позволяет:

- визуализировать в системной панели состояние «вирусной погоды»;
- подписываться и отказываться от подписки на новостные каналы «Лаборатории Касперского»;
- получать с заданной периодичностью новости по каждому подписанному каналу; также осуществляется оповещение о появлении непрочитанных новостей;
- просматривать новости по подписанным каналам;
- просматривать списки каналов и их состояние;
- открывать в браузере страницы с подробным текстом новостей.

Новостной Агент работает под управлением операционной системы Microsoft Windows и может использоваться как отдельная программа, так и входить в состав различных интегрированных решений «Лаборатории Касперского».

Kaspersky® OnLine Scanner

Программа представляет собой бесплатный сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера в онлайн-режиме. Kaspersky OnLine Scanner выполняется непосредственно в браузере. Таким образом, пользователи могут максимально оперативно получать ответ на вопросы, связанные с

заражением вредоносными программами. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- сохранять отчеты о результатах проверки в форматах txt и html.

Kaspersky® OnLine Scanner Pro

Программа представляет собой подписной сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера и лечение зараженных файлов в онлайн-режиме. Kaspersky OnLine Scanner Pro выполняется непосредственно в браузере. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- лечить обнаруженные зараженные объекты;
- сохранять отчеты о результатах проверки в форматах txt и html.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 – комплексное решение для защиты персонального компьютера от основных информационных угроз – вирусов, хакеров, спама и шпионских программ. Единый пользовательский интерфейс обеспечивает настройку и управление всеми компонентами решения.

Функции антивирусной защиты включают в себя:

- *антивирусную проверку почтового трафика* на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих) независимо от используемой почтовой программы. Для популярных почтовых программ Microsoft Office Outlook, Microsoft Outlook Express и The Bat! предусмотрены плагины и лечение вирусов в почтовых базах;
- *проверку интернет-трафика*, поступающего по HTTP-протоколу, в режиме реального времени;
- *защиту файловой системы*: антивирусной проверке могут быть подвергнуты любые отдельные файлы, папки и диски. Также возможна проверка только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows;
- *проактивную защиту*: программа осуществляет постоянное наблюдение за активностью приложений и процессов, запущенных в оперативной памяти компьютера, предотвращает опас-

ные изменения файловой системы и реестра, а также восстанавливает систему после вредоносного воздействия.

Защита от интернет-мошенничества обеспечивается благодаря распознаванию фишинговых атак, что позволяет предотвратить утечку вашей конфиденциальной информации (в первую очередь паролей, номеров банковских счетов и карт, а также блокированию выполнения опасных скриптов на веб-страницах, всплывающих окон и рекламных баннеров). Функция *блокирования автоматического дозвона на платные ресурсы интернета* помогает идентифицировать программы, которые пытаются использовать ваш модем для скрытого соединения с платными телефонными сервисами, и блокировать их работу. Модуль *Защита конфиденциальных данных* обеспечивает защиту от несанкционированного доступа и передачи информации личного характера. Функция *Родительский контроль* обеспечивает контроль доступа пользователей компьютера к интернет-ресурсам.

Kaspersky Internet Security 6.0 *фиксирует попытки сканирования портов вашего компьютера*, часто предшествующие сетевым атакам, и успешно отражает наиболее распространенные типы сетевых атак. На *основе заданных правил* программа осуществляет контроль всех сетевых взаимодействий, отслеживая все *входящие и исходящие пакеты данных*. Режим *невидимости предотвращает обнаружение компьютера извне*. При переключении в этот режим запрещается вся сетевая деятельность, кроме предусмотренных правилами исключений, которые определяются самим пользователем.

В программе применяется комплексный подход к фильтрации входящих почтовых сообщений на наличие спама:

- проверка по «черным» и «белым» спискам адресатов (включая адреса фишинговых сайтов);
- проверка фраз в тексте письма;
- анализ текста письма с помощью самообучающегося алгоритма;
- распознавание спама в виде изображений.

Антивирус Касперского® Mobile

Антивирус Касперского Mobile обеспечивает антивирусную защиту мобильных устройств, работающих под управлением операционных систем Symbian OS и Microsoft Windows Mobile. Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- *проверку по требованию* памяти мобильного устройства, карт памяти, отдельной папки либо конкретного файла. При обнаружении зараженного объекта он помещается на карантин или удаляется;

- *постоянную защиту*: автоматически проверяются все входящие или изменяющиеся объекты, а также файлы при попытке доступа к ним;
- *защиту от sms- и mms-спама*.

Антивирус Касперского для файловых серверов

Программный продукт обеспечивает надежную защиту файловых систем серверов под управлением операционных систем Microsoft Windows, Novell NetWare, Linux и Samba от всех видов вредоносных программ. В состав программного продукта входят следующие приложения «Лаборатории Касперского»:

- Kaspersky Administration Kit.
- Антивирус Касперского для Windows Server.
- Антивирус Касперского для Linux File Server.
- Антивирус Касперского для Novell Netware.
- Антивирус Касперского для Samba Server.

Преимущества и функциональные возможности:

- *защита файловых систем серверов в режиме реального времени*: все файлы серверов проверяются при попытке их открытия и сохранения на сервере.
- *предотвращение вирусных эпидемий*;
- *проверка по требованию* всей файловой системы или отдельных ее папок и файлов;
- *применение технологий оптимизации* при проверке объектов файловой системы сервера;
- *восстановление системы после заражения*;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *соблюдение баланса загрузки системы*;
- *формирование списка доверенных процессов*, чья активность на сервере не подвергается контролю со стороны программного продукта;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *хранение резервных копий зараженных и удаленных объектов* на тот случай, если потребуется их восстановление;

- *изоляция подозрительных объектов* в специальном хранилище;
- *оповещения о событиях* в работе программного продукта администратора системы;
- *ведение детальных отчетов*;
- *автоматическое обновление баз* программного продукта.

Kaspersky Open Space Security

Kaspersky Open Space Security – это программный продукт, реализующий новый подход к безопасности современных корпоративных сетей любого масштаба, обеспечивающий централизованную защиту информационных систем, а также поддержку удаленных офисов и мобильных пользователей.

Программный продукт включает в себя четыре продукта:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Рассмотрим подробнее каждый продукт.

Kaspersky WorkSpace Security – это продукт для централизованной защиты рабочих станций в корпоративной сети и за ее пределами от всех видов современных интернет-угроз: вирусов, шпионских программ, хакерских атак и спама.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама*;
- *проактивная защита* от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- *отмена вредоносных изменений в системе*;
- *защита от фишинг-атак и нежелательной почтовой корреспонденции*;
- *динамическое перераспределение ресурсов* при полной проверке системы;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;

- *поддержка Cisco® NAC (Network Admission Control);*
- *проверка электронной почты и интернет-трафика в режиме реального времени;*
- *блокирование всплывающих окон и рекламных баннеров при работе в интернете;*
- *безопасная работа в сетях любого типа, включая Wi-Fi;*
- *средства для создания диска аварийного восстановления, позволяющего восстановить систему после вирусной атаки;*
- *развитая система отчетов о состоянии защиты;*
- *автоматическое обновление баз;*
- *полноценная поддержка 64-битных операционных систем;*
- *оптимизация работы программного продукта на ноутбуках (технология Intel® Centrino® Duo для мобильных ПК);*
- *возможность удаленного лечения (технология Intel® Active Management, компонент Intel® vPro™).*

Kaspersky Business Space Security обеспечивает оптимальную защиту информационных ресурсов компании от современных интернет-угроз. Kaspersky Business Space Security защищает рабочие станции и файловые серверы от всех видов вирусов, троянских программ и червей, предотвращает вирусные эпидемии, а также обеспечивает сохранность информации и мгновенный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC (Network Admission Control);*
- *защита рабочих станций и файловых серверов от всех видов интернет-угроз;*
- *использование технологии iSwift для исключения повторных проверок в рамках сети;*
- *распределение нагрузки между процессорами сервера;*
- *изоляция подозрительных объектов рабочих станций в специальном хранилище;*
- *отмена вредоносных изменений в системе;*

- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *проверка электронной почты и интернет-трафика* в режиме реального времени;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- *защита при работе в беспроводных сетях Wi-Fi*;
- *технология самозащиты антивируса от вредоносных программ*;
- *изоляция подозрительных объектов* в специальном хранилище;
- *автоматическое обновление баз*.

Kaspersky Enterprise Space Security

Программный продукт включает компоненты для защиты рабочих станций и серверов совместной работы от всех видов современных интернет-угроз, удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и мгновенный безопасный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *защита рабочих станций и серверов от вирусов, троянских программ и червей*;
- *защита почтовых серверов Sendmail, Qmail, Postfix и Exim*;
- *проверка всех сообщений на сервере Microsoft Exchange*, включая общие папки;
- *обработка сообщений, баз данных и других объектов серверов Lotus Domino*;
- *защита от фишинг-атак и нежелательной почтовой корреспонденции*;
- *предотвращение массовых рассылок и вирусных эпидемий*;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;

- *поддержка Cisco® NAC (Network Admission Control);*
- *проактивная защита рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;*
- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *безопасная работа в беспроводных сетях Wi-Fi;*
- *проверка интернет-трафика в режиме реального времени;*
- *отмена вредоносных изменений в системе;*
- *динамическое перераспределение ресурсов при полной проверке системы;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *система отчетов о состоянии системы защиты;*
- *автоматическое обновление баз.*

Kaspersky Total Space Security

Решение контролирует все входящие и исходящие потоки данных – электронную почту, интернет-трафик и все сетевые взаимодействия. Продукт включает компоненты для защиты рабочих станций и мобильных устройств, обеспечивает мгновенный и безопасный доступ пользователей к информационным ресурсам компании и сети Интернет, а также гарантирует безопасные коммуникации по электронной почте.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама на всех уровнях корпоративной сети: от рабочих станций до интернет-шлюзов;*
- *проактивная защита рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;*
- *защита почтовых серверов и серверов совместной работы;*
- *проверка интернет-трафика (HTTP/FTP), поступающего в локальную сеть, в режиме реального времени;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *блокирование доступа с зараженных рабочих станций;*

- *предотвращение вирусных эпидемий;*
- *централизованные отчеты о состоянии защиты;*
- *удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;*
- *поддержка Cisco® NAC (Network Admission Control);*
- *поддержка аппаратных прокси-серверов;*
- *фильтрация интернет-трафика по списку доверенных серверов, типам объектов и группам пользователей;*
- *использование технологии iSwift для исключения повторных проверок в рамках сети;*
- *динамическое перераспределение ресурсов при полной проверке системы;*
- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *безопасная работа пользователей в сетях любого типа, включая WiFi;*
- *защита от фишинг-атак и нежелательной почтовой корреспонденции;*
- *возможность удаленного лечения (технология Intel® Active Management, компонент Intel® vPro™);*
- *отмена вредоносных изменений в системе;*
- *технология самозащиты антивируса от вредоносных программ;*
- *полноценная поддержка 64-битных операционных систем;*
- *автоматическое обновление баз.*

Kaspersky Security для почтовых серверов

Программный продукт для защиты почтовых серверов и серверов совместной работы от вредоносных программ и спама. Продукт включает в себя приложения для защиты всех популярных почтовых серверов: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix и Exim, а также позволяет организовать выделенный почтовый шлюз. В состав решения входят:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.

- Антивирус Касперского для Lotus Notes/Domino.
- Антивирус Касперского для Microsoft Exchange.
- Антивирус Касперского для Linux Mail Server.

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ;*
- *фильтрация нежелательной почтовой корреспонденции;*
- *проверка входящих и исходящих почтовых сообщений и вложений;*
- *антивирусная проверка всех сообщений на сервере Microsoft Exchange, включая общие папки;*
- *проверка сообщений, баз данных и других объектов серверов Lotus Notes/Domino;*
- *фильтрация сообщений по типам вложений;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *удобная система управления программным продуктом;*
- *предотвращение вирусных эпидемий;*
- *мониторинг состояния системы защиты с помощью уведомлений;*
- *система отчетов о работе приложения;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *автоматическое обновление баз.*

Kaspersky Security для интернет-шлюзов

Программный продукт обеспечивает безопасный доступ к сети Интернет для всех сотрудников организации, автоматически удаляя вредоносные и потенциально опасные программы из потока данных, поступающего в сеть по протоколам HTTP/FTP. В состав продукта входят:

- Kaspersky Administration Kit.
- Антивирус Касперского для Proxy Server.
- Антивирус Касперского для Microsoft ISA Server.
- Антивирус Касперского для Check Point FireWall-1.

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ;*
- *проверка интернет-трафика (HTTP/FTP) в режиме реального времени;*
- *фильтрация интернет-трафика по списку доверенных серверов, типам объектов и группам пользователей;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *удобная система управления;*
- *система отчетов о работе приложения;*
- *поддержка аппаратных прокси-серверов;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *автоматическое обновление баз.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam – первый российский программный комплекс для защиты от нежелательных писем (спама) для предприятий средних и малых масштабов. Продукт сочетает революционные технологии лингвистического анализа текстов, все современные методы фильтрации электронной почты (включая списки DNS Black List и формальные признаки письма) и уникальный набор сервисов, которые позволяют пользователям распознать и уничтожить до девяноста пяти процентов нежелательного трафика.

Kaspersky® Anti-Spam представляет собой фильтр, который устанавливается на «входе» в сеть предприятия и проверяет входящий поток писем на предмет обнаружения спама. Продукт совместим с любой почтовой системой, используемой в сети заказчика, и может быть установлен как на уже существующий почтовый сервер, так и на выделенный.

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению баз контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории. Обновления баз выпускаются каждые 20 минут.

Антивирус Касперского® для MIMESweeper

Антивирус Касперского® для MIMESweeper обеспечивает высокоскоростную антивирусную проверку трафика на серверах, использующих Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Программа выполнена в виде плагина (модуля расширения) и осуществляет в режиме реального времени антивирусную проверку и обработку входящих и исходящих почтовых сообщений.

С.2. Наши координаты

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.

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-8700, +7 (495) 645-79-39
Экстренная круглосуточная помощь:	+7 (495) 797-8707, +7 (495) 645-79-29
Поддержка пользователей персональных продуктов и Business Optimal:	+7 (495) 797-8707, +7 (495) 645-79-29 (с 10 до 19 часов) http://support.kaspersky.ru/helpdesk.html
Поддержка пользователей Corporate Suite:	Телефоны и электронный адрес предоставляются при покупке Corporate Suite в зависимости от пакета технической поддержки.
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)

Департамент продаж:	+7 (495) 797-8700, +7 (495) 645-79-39 sales@kaspersky.com
Общая информация:	+7 (495) 797-8700, +7 (495) 645-79-39 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru