ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского 6.0 для Windows Workstations

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

АНТИВИРУС КАСПЕРСКОГО 6.0
ДЛЯ WINDOWS WORKSTATIONS

Руководство пользователя

Тел., факс: +7 (495) 797-87-00, +7 (495) 645-79-39,
+7 (495) 956-70-00
http://www.kaspersky.ru

Дата редакции: август 2007 года

Содержание

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 деятель-

ности 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 использующегося 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 запускаемые 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 несанкционированные 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 случает 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 удаленного компьютера, выведение системы из строя или получение полного контроля над ресурсами компьютера. Подробное описание видов атак, блокируемых Антивирусом Касперского, представлено в разделе 12.9 на стр. 172.

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) инициируют 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 обновляемой базы сигнатур угроз. Для реализации данного метода необходимо хотя бы одно заражение, чтобы добавить сигнатуру угрозы в базу 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. 5.2 на стр. 67).

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 сигнатуры угроз и модули приложения (см. п. 5.6 на стр. 71). 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, поскольку 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 антивирусных 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. 5.2 на стр. 67).

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 сигнатуры угроз, входящие в состав приложения (см. п. 5.6 на стр. 71). Обновление можно проводить несколько

раз в день при возникновении вирусных эпидемий – в таких ситуациях сигнатуры угроз 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. Если вы не установили компонент Анти-Хакер, рекомендуется сделать это, чтобы защитить компьютер при работе в интернете.

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. 5.4 на стр. 69).

- 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, 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. 17.10 на стр. 272), 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 пунктом **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 6.0

Антивирус Касперского 6.0 – это новое поколение решений по защите информации.

Основное отличие Антивируса Касперского 6.0 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 6.0

Антивирус Касперского 6.0 – 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 спама и защиту от хакерских атак. Новые модули позволяют защищать от неизвестных угроз, от фишинга и маскировщиков вредоносной активности.

Больше не нужно устанавливать несколько продуктов на компьютер, чтобы обеспечить себе полноценную защиту. Достаточно просто установить Антивирус Касперского 6.0.

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

Рассмотрим детально нововведения Антивируса Касперского 6.0.

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. 129) – основное преимущество приложения. Его работа построена на анализе поведения приложений, установленных на вашем компьютере, на контроле изменений системного реестра, отслеживании выполнения макросов и борьбе со скрытыми угрозами. В работе компонента ис-

пользуется 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.

- Обеспечивается защита от руткитов, программ автодозвона на платные веб-сайты, блокировка баннеров, всплывающих окон и вредоносных сценариев, загружаемых с веб-страниц в интернете, а также распознавание фишинг-сайтов.

- 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, заражение которых может привести к серьезным последствиям, представлена отдельной задачей. Вы можете настроить автоматический запуск этой задачи каждый раз при старте системы.

- Значительно улучшена защита электронной корреспонденции, как от вредоносных программ, так и от спама. Приложение проверяет на вирусы и спам почтовый трафик на следующих протоколах:

    - IMAP, SMTP, POP3, независимо от используемого вами почтового клиента;

    - NNTP (только проверка на вирусы), 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 настраи-

вать защиту почты непосредственно в почтовом клиенте, как от вирусов, так и от спама.

- Обучение Анти-Спама производится на письмах вашего почтового ящика, что позволяет учесть все особенности вашей работы с письмами и максимально гибко настроить обнаружение нежелательной корреспонденции. В основу обучения положен алгоритм iBayes. Кроме того, вы можете составлять «черные» и «белые» списки адресатов и ключевых фраз, на основании которых производится обнаружение спама.

  В процессе работы Анти-Спама используется база фишинга. Она позволяет отфильтровывать письма, целью которых является получение конфиденциальной информации финансового характера.

- Приложение обеспечивает фильтрацию входящего и исходящего трафика, отслеживает и предотвращает угрозы распространенных сетевых атак, позволяет работать в сети в режиме «невидимости».

- При работе в сети вы теперь самостоятельно можете определять, какой сети можно доверять на все 100 процентов, а в какой – соблюдать максимальную осторожность.

- Расширена функция оповещения пользователя (см. п. 17.11.1 на стр. 277) 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 приложения, 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.

- Добавлена возможность централизованного удаленного управления системой защиты с помощью дополнительного административного интерфейса под управлением Kaspersky Administration Kit.

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, сопровождает свою работу комментариями и советами, включает подробную справку.

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 Антивирус 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 сигнатур угроз.
- 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 защиты (см. п. 2.2.1 на стр. 27), 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. 29), посредством которых выполняется проверка компьютера или отдельных файлов, папок, дисков или областей, на присутствие вирусов.
- Сервисные функции (см. п. 2.2.3 на стр. 30), обеспечивающие информационную поддержку в работе с приложением и позволяющие расширить ее функциональность.

2.2.1. Компоненты защиты

Защита вашего компьютера в реальном времени обеспечивается следующими компонентами защиты:

Файловый Антивирус

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

Файловый Антивирус – компонент, контролирующий файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на вашем компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается Антивирусом Касперского, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен Антивирусом. Если же файл по каким-либо причинам невозможно вылечить, он будет удален, при этом копия файла будет сохранена в резервном хранилище (см. п. 17.2 на стр. 244) или помещена на карантин (см. п. 17.1 на стр. 240).

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.

Анти-Шпион

В последнее время широкое распространение получили программы, производящие несанкционированный показ материалов рекламного характера (баннеры, всплывающие окна), программы несанкционированного дозвона на платные интернет-ресурсы, различные средства удаленного администрирования и мониторинга, программы-шутки и т.д.

Анти-Шпион отслеживает данные действия на вашем компьютере и блокирует их выполнение. Например, компонент блокирует показ баннеров и всплывающих окон, мешающих пользователю при работе с веб-ресурсами, блокирует работу программ, пытающихся осуществить несанкционированный пользователем дозвон, анализирует веб-страницы на предмет фишинг-мошенничества.

Анти-Хакер

Для вторжения на ваш компьютер хакеры используют любую возможную «лазейку», будь то открытый порт, передача информации с компьютера на компьютер и т.д.

Анти-Хакер – компонент, предназначенный для защиты вашего компьютера при работе в интернете и других сетях. Он контролирует исходящие и входящие соединения, проверяет порты и пакеты данных.

Анти-Спам

Не являясь источником прямой угрозы, нежелательная корреспонденция (спам) увеличивает нагрузку на почтовые серверы, засоряет почтовый ящик пользователя, ведет к потере времени и тем самым наносит значительный финансовый урон.

Компонент *Анти-Спам* встраивается в установленный на вашем компьютере почтовый клиент и контролирует все поступающие почтовые сообщения на предмет спама. Все письма, содержащие спам, помечаются специальным заголовком. Предусмотрена также возможность настройки Анти-Спама на обработку спама (автоматическое удаление, помещение в специальную папку и т.д.).

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 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.

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. 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.

Обновление

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

Сервис копирования обновлений позволяет сохранять обновления баз сигнатур угроз, сетевых атак и сетевых драйверов, 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.

Файлы данных

В процессе работы приложения по каждому компоненту защиты, задаче поиска вирусов или обновлению приложения формируется отчет. Он содержит информацию о выполненных операциях и результаты работы. Пользуясь функцией *Отчеты*, вы всегда можете 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.

Аварийный диск

В состав Антивируса Касперского включен специальный сервис, позволяющий создавать диск аварийного восстановления системы.

Создание такого диска полезно на случай повреждения системных файлов в результате вирусной атаки и невозможности выполнить загрузку операционной системы. В этом случае, используя аварийный диск, вы сможете загрузить компьютер и восстановить систему до состояния, предшествующего вредоносному воздействию.

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», просмотреть список часто задаваемых вопросов, ответы на которые, возможно, помогут в решении вашей проблемы. Кроме того, заполнив, специальную форму на сайте, вы можете отправить в Службу технической поддержки сообщение об ошибке или отзыв о работе приложения.

Также для вас доступна Служба технической поддержи он-лайн 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 6.0, компьютер должен удовлетворять следующим минимальным требованиям:

Общие требования:

- 50 МБ свободного места на жестком диске.
- CD-ROM (для установки Антивируса Касперского 6.0 с дистрибутивного CD-диска).
- Microsoft Internet Explorer 5.5 или выше (для обновления сигнатур угроз и модулей приложения через интернет).
- Microsoft Windows Installer 2.0.

Microsoft Windows 98(SE), Microsoft Windows ME, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

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

Microsoft Windows 2000 Professional (Service Pack 4 или выше), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 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 приложения входят:

- Запечатанный конверт с установочным компакт-диском, на котором записаны файлы приложения.
- Лицензионный ключ, включенный в состав дистрибутива или записанный на специальную дискету, либо 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**.

Лицензионный ключ либо 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 приложением.

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 лицензии можете получать следующие услуги:

- предоставление новых версий данного приложения;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного приложения, 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 6.0

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

- локальная установка – установка приложения на отдельном компьютере. Для запуска и проведения установки требуется непосредственный доступ к данному компьютеру. Локальная установка может быть проведена в одном из двух режимов:
    - интерактивном, с помощью мастера установки приложения (см. п. 3.1 на стр. 36), данный режим требует участия пользователя в процессе установки;
    - неинтерактивном, запуск установки приложения в данном режиме выполняется из командной строки и не требует участия пользователя в процессе установки (см. п. 3.3 на стр. 50).
- удаленная установка – установка приложения на компьютеры сети, выполняемая удаленно с рабочего места администратора с использованием:
    - программного комплекса Kaspersky Administration Kit (см. «Руководство по внедрению Kaspersky Administration Kit»);
    - групповых доменных политик Microsoft Windows Server 2000/2003 (см. п. 3.4 на стр. 51).

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

В случае если у вас уже установлен Антивирус Касперского версии 5.0, после запуска процедуры установки будет проведено обновление до версии 6.0 с удалением предыдущей версии (подробнее см. п. 3.5 на стр. 53). Обновление с одной сборки на другую в рамках версии 6.0 выполняется без каких-либо особенностей.

3.1. Процедура установки с помощью мастера установки

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

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

Шаг 4. Выбор каталога установки

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

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

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

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

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

Шаг 5. Использование параметров приложения, сохраненных с предыдущей установки

На данном этапе вам будет предложено определить, хотите ли вы использовать в работе приложения параметры защиты, сигнатуры угроз и базу Анти-Спама, если таковые были сохранены на вашем компьютере при удалении предыдущей версии Антивируса Касперского 6.0.

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 ком-

пьютере сигнатуры угроз, вы можете подключить их для использования в устанавливаемой версии. Для этого установите флажок **Сигнатуры угроз**. Сигнатуры угроз, 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 работы приложения**.

Также рекомендуется воспользоваться базой Анти-Спама, если таковая была сохранена при удалении предыдущей версии приложения. Это позволит вам избежать процедуры обучения Анти-Спама. Чтобы учесть уже сформированную вами базу, установите флажок **Базу Анти-Спама**.

Шаг 6. Выбор типа установки

На данном этапе вам нужно определить полноту установки приложения на ваш компьютер. Предусмотрено три варианта установки:

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

Выборочная. В данном случае вам будет предложено выбрать, какие компоненты приложения вы хотите установить на ваш компьютер. Подробнее см. Шаг 7.

Компоненты антивирусной защиты. Такой вариант предполагает установку только компонентов, обеспечивающих антивирусную защиту вашего компьютера. Компоненты Анти-Хакер, Анти-Спам и Анти-Шпион установлены не будут.

Для выбора типа установки нажмите на соответствующую кнопку.

Шаг 7. Выбор компонентов приложения для установки

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

При выборочной установке вам нужно определить список компонентов Антивируса Касперского, которые вы хотите установить. По умолчанию для установки выбраны все компоненты защиты, компонент поиска вирусов, а также коннектор к Агенту администрирования для удаленного управления приложением через Kaspersky Administration Kit.

Для того чтобы выбрать компонент для последующей установки, нужно открыть меню по левой клавише мыши на значке рядом с именем компонента и выбрать пункт **Компонент будет установлен на локальный жесткий**

диск. Подробнее о том, какую защиту обеспечивает выбранный компонент и сколько места на диске требуется для его установки, вы можете прочесть в нижней части данного окна программы установки.

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 8. Отключение сетевого экрана Microsoft Windows

Данный шаг выполняется только в том случае, если Антивирус Касперского устанавливается на компьютер с включенным сетевым экраном, и в числе устанавливаемых компонентов присутствует Анти-Хакер.

На данном этапе установки Антивируса Касперского вам предлагается отключить сетевой экран операционной системы Microsoft Windows, поскольку входящий в состав Антивируса Касперского компонент Анти-Хакер обеспечивает полную защиту вашей работы в сети, и нет необходимости в дополнительной защите средствами операционной системы.

Если вы хотите использовать Анти-Хакер в качестве основного средства защиты при работе в сети, нажмите на кнопку **Далее**. Сетевой экран Microsoft Windows будет автоматически отключен.

Если вы хотите защищать свой компьютер с помощью сетевого экрана Microsoft Windows, выберите вариант **Использовать сетевой экран Microsoft Windows**. В этом случае компонент Анти-Хакер будет установлен, но отключен во избежание конфликтов в работе приложений.

Шаг 9. Поиск других антивирусных приложений

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 приложений 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.

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

Шаг 10. Завершающая подготовка к установке приложения

На данном этапе вам будет предложено произвести завершающую подготовку к установке приложения на ваш компьютер.

При первоначальной установке Антивируса Касперского 6.0 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.

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.

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

Внимание!

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

Шаг 11. Завершение процедуры установки

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

Для запуска мастера первоначальной настройки приложения нажмите на кнопку **Далее** (см. п. 3.2 на стр. 40).

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

3.2. Мастер первоначальной настройки

Мастер настройки Антивируса Касперского 6.0 запускается по завершении процедуры установки приложения. Его задача – помочь вам провести пер-

вичную 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 **Готово**. 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. 17.13 на стр. 285).

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 6.0. Это могут быть объекты карантина, резервного хранилища либо параметры защиты.

Для того чтобы использовать эти данные в версии 6.0 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 полнофункциональной работы приложения, а также дополнительные сведения:

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

3.2.2.1. Выбор способа активации приложения

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

- **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 лицензионный ключ, обеспечивающий доступ к полной функциональности приложения на весь период действия лицензии.
- **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 лицензионный ключ со сроком действия, ограниченным лицензией для пробной версии приложения.
- **Использовать полученный ранее лицензионный ключ**. Активируйте приложение с помощью полученного ранее файла лицензионного ключа для Антивируса Касперского 6.0.
- **Активировать приложение позже**. При выборе этого варианта этап активации приложения будет пропущен. Антивирус Касперского 6.0 будет установлен на ваш компьютер, вам будут доступны все функции приложения, за исключением обновления (обновить сигнатуры угроз вы сможете только один раз после установки приложения).

При выборе первых двух вариантов активация приложения осуществляется через веб-сервер «Лаборатории Касперского», для соединения с которым требуется подключение к интернету. Перед началом активации проверьте и, при необходимости, измените параметры сетевого соединения (см. п. 16.4.3 на стр. 234) в окне, открывающемся по кнопке **Параметры LAN**. Для получения более подробной информации о настройке сетевых параметров обратитесь к вашему системному администратору или интернет-провайдеру.

Если на момент установки соединение с интернетом отсутствует, вы можете провести активацию позже (см. п. 17.5 на стр. 262) из интерфейса приложения либо, выйдя в интернет с другого компьютера, получить лицензионный ключ по коду активации, зарегистрировавшись на веб-сайте Службы технической поддержки «Лаборатории Касперского».

3.2.2.2. Ввод кода активации

Для активации приложения требуется ввести код активации. При покупке приложения через интернет код активации отправляется вам по электрон-

ной почте. В случае покупки приложения в коробке, код активации указан на конверте с установочным диском.

Код активации представляет собой последовательность цифр и букв, разделенных дефисами на четыре блока по пять символов, без пробелов. Например, 11AA1-11AAA-1AA11-1A111. Обратите внимание, что код должен вводиться латинскими символами.

В нижней части окна укажите вашу контактную информацию: фамилию, имя, отчество, адрес электронной почты, страну и город проживания. Данная информация может потребоваться для идентификации зарегистрированного пользователя, если, например, ключ был утрачен или похищен. В данном случае на основании контактных данных вы сможете получить другой лицензионный ключ.

3.2.2.3. Получение лицензионного 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 лицензионного 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 о лицензии.

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

3.2.2.4. Выбор файла лицензионного ключа

Если у вас имеется файл лицензионного ключа для Антивируса Касперского 6.0, 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 информация о лицензии: имя владельца, номер лицензии, ее тип (коммерческая, для бета-тестирования, пробная и т.д.), а также дата окончания срока действия ключа.

3.2.2.5. Завершение активации приложения

Мастер настройки информирует вас об успешном завершении активации приложения. Кроме того, приводится информация об установленном лицензионном ключе: имя владельца, номер лицензии, ее тип (коммерческая, для бета-тестирования, пробная 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, а также несанкционированные действия в сети.

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 режим обучения Анти-Хакера** – запрашивать подтверждение действий пользователя при попытках программ, установленных на вашем компьютере, установить соединение с некоторым сетевым ресурсом. Вы можете разрешить либо запретить данное соединение, настроить правила работы Анти-Хакера для данной программы. При отключении режима обучения Анти-Хакер работает в режиме минимальной защиты, то есть всем приложениям разрешен доступ к сетевым ресурсам.
- **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 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 сигнатур угроз 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 Антивирус скачивает их и устанавливает на компьютер. Такой режим используется по умолчанию.

Каждые 2 часа (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию. Параметры расписания можно установить в окне, открывающемся по кнопке **Изменить**.

Вручную. В этом случае вы будете самостоятельно запускать обновление приложения.

Обратите внимание, что базы сигнатур угроз 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 (установить сетевые параметры, выбрать ресурс, с которого будет происходить обновление, настроить запуск обновления от имени определенной учетной записи, а также включить сервис копирования обновлений в локальный источник), нажмите на кнопку **Настройка**.

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, открывающемся 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, открывающемся 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, открывающемся 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:**
  - **Сохранение 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 поиска вирусов** – запрос пароля при попытке пользователя приостановить или выключить полностью работу какого-либо компонента защиты либо задачи поиска вирусов.

3.2.7. Настройка параметров работы Анти-Хакера

Анти-Хакер – компонент Антивируса Касперского, обеспечивающий безопасность работы вашего компьютера в локальных сетях и интернете. На данном этапе мастер настройки предлагает вам сформировать ряд правил, которыми Анти-Хакер будет руководствоваться при анализе сетевой активности вашего компьютера.

3.2.7.1. Определение статуса зоны безопасности

На данном этапе мастер настройки проводит анализ сетевого окружения вашего компьютера. По результатам анализа все сетевое пространство делится на условные зоны:

Интернет – глобальная сеть Интернет. В данной зоне Антивирус Касперского работает как персональный сетевой экран. При этом вся сетевая активность регламентируется правилами для пакетов и приложений, созданными по умолчанию для обеспечения максимальной безопасности. Вы не можете изменять условия защиты

при работе в данной зоне, кроме как включить режим невидимости компьютера для дополнительной безопасности.

Зоны безопасности – некоторые условные зоны, зачастую совпадающие с подсетями, в которые включен ваш компьютер (это могут быть локальные подсети дома или на работе). По умолчанию данные зоны считаются зонами средней степени риска при работе в них. Вы можете изменять статус данных зон исходя из степени доверия той или иной подсети, а также настраивать правила для пакетов и приложений.

Все обнаруженные зоны представлены в списке. Для каждой из них дано описание, указаны адрес и маска подсети, а также статус, на основании которого будет разрешена либо запрещена та или иная сетевая активность в рамках работы компонента Анти-Хакер:

- **Интернет**. Этот статус по умолчанию присваивается сети Интернет, поскольку при работе в ней компьютер подвержен любым возможным типам угроз. Также данный статус рекомендуется выбирать для сетей, не защищенных какими-либо антивирусными приложениями, сетевыми экранами, фильтрами и т.д. При выборе этого статуса обеспечивается максимальная безопасность работы компьютера в данной зоне, а именно:

  - блокируется любая сетевая NetBios-активность в рамках подсети;
  - запрещается выполнение правил для приложений и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

  Даже если вы создали папку общего доступа, информация, содержащаяся в ней, не будет доступна пользователям подсети с таким статусом. Кроме того, при выборе данного статуса вы не сможете получить доступ к файлам и принтерам на других компьютерах сети.

- **Локальная сеть**. Этот статус присваивается по умолчанию большинству зон безопасности, обнаруженных при анализе сетевого окружения компьютера, за исключением сети Интернет. Рекомендуется применять этот статус для зон со средней степенью риска работы в них (например, для внутренней корпоративной сети). При выборе данного статуса разрешается:

  - любая сетевая NetBios-активность в рамках подсети;
  - выполнение правил для приложений и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

  Выбирайте этот статус, если вы хотите предоставить доступ к некоторым каталогам или принтерам на вашем компьютере, но запретить любую другую внешнюю активность.

- **Доверенная**. Этот статус рекомендуется применять только для абсолютно безопасной, по вашему мнению, зоны, при работе в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. При выборе такого статуса будет разрешена любая сетевая активность. Даже если установлен уровень Максимальной защиты и созданы запрещающие правила, они не будут действовать для удаленных компьютеров доверенной зоны.

Для сети со статусом **Интернет** вы можете для дополнительной безопасности использовать *режим невидимости*. В этом режиме разрешена только сетевая активность, инициируемая с вашего компьютера. Фактически это означает, что ваш компьютер становится «невидимым» для внешнего окружения. В то же время на вашу работу в интернете режим не оказывает никакого влияния.

Не рекомендуется использовать режим невидимости, если компьютер используется в качестве сервера (например, почтового, http-сервера). Иначе, компьютеры, обращающиеся к данному серверу, не будут видеть его в сети.

Чтобы изменить статус зоны либо включить/ отключить режим невидимости, выберите ее в списке и в блоке **Описание**, расположенном под списком, воспользуйтесь соответствующими ссылками. Аналогичные действия, а также редактирование адреса и маски подсети можно выполнить в окне **Параметры зоны**, открывающемся по кнопке **Изменить**.

При просмотре списка зон вы можете добавить в него новую, для этого воспользуйтесь кнопкой **Найти**. Анти-Хакер произведет поиск доступных зон и, если таковые будут обнаружены, предложит вам определить их статус. Кроме того, вы можете добавить новую зону в список вручную (например, в случае, когда вы включаете мобильный компьютер в новую сеть). Для этого воспользуйтесь кнопкой **Добавить** и укажите требующуюся информацию в окне **Параметры зоны**.

Чтобы удалить сеть из списка, воспользуйтесь кнопкой **Удалить**.

3.2.7.2. Формирование списка сетевых приложений

Мастер настройки анализирует установленное на вашем компьютере программное обеспечение и формирует список приложений, использующих для своей работы сеть.

Для каждого из таких приложений Анти-Хакер создает правило, регламентирующее сетевую активность. Правила применяются на основе сформированных в «Лаборатории Касперского» и включенных в поставку продукта шаблонов наиболее распространенных приложений, использующих сеть.

Список сетевых приложений и правила для них вы можете посмотреть в окне настройки Анти-Хакера, которое открывается по кнопке **Список**.

В качестве дополнительной защиты рекомендуется отключить кеширование доменных имен при работе с интернет-ресурсами. Этот сервис значительно сокращает время соединения вашего компьютера с нужным интернет-ресурсом, однако в то же время является опасной уязвимостью, используя которую злоумышленники могут организовать канал утечки данных, который невозможно будет отследить с помощью сетевого экрана. Поэтому для повышения уровня безопасности вашего компьютера мы рекомендуем отключать сохранение информации о доменных именах в кеше.

3.2.8. Завершение работы мастера настройки

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

Вы можете отложить перезагрузку компьютора, 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 6.0 для Windows Workstations, наберите в командной строке:

```
msiexec /i <имя_пакета>
```

Будет запущен мастор установки (см. п. 3.1 на стр. 36). По завершении установки приложения, необходимо перезагрузить компьютер.

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

```
msiexec /i <имя_пакета> /qn
```

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

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

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

Чтобы установить приложение с указанием пароля, подтверждающего право на удаление приложения, наберите:

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

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

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

При установке Антивируса Касперского в неинтерактивном режиме поддерживается чтение файла *setup.ini*, содержащего общие параметры установки приложения (см. п. А.4 на стр. 335), конфигурационного файла *install.cfg* (см. п. 18.7 на стр. 300), а также файла лицензионного ключа. Обратите внимание, что данные файлы должны быть расположены в одном каталоге с дистрибутивом Антивируса Касперского.

3.4. Процедура установки через Редактор объектов групповой политики (Group Policy Object)

Данная возможность поддерживается на компьютерах с операционной ситемой Microsoft Windows 2000 и выше.

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

3.4.1. Установка приложения

Для установки Антивируса Касперского:

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

Дополнительно в данную директорию можно поместить файл *setup.ini*, содержащий перечень параметров установки Антивируса Касперского (подробное описание параметров данного файла см. в п. А.4 на стр. 335), конфигурационный файл *install.cfg* (см. п. 18.7 на стр. 300), а также файл ключа.

2. Откройте **Редактор объектов групповой политики** через стандартную консоль MMC (подробную информацию о работе с Редактором см. в справочной системе к Microsoft Windows Server).

3. Создайте новый пакет. Для этого в дереве консоли выберите **Объект групповой политики/ Конфигурация компьютера/ Конфигурация программ/ Установка программного обеспечения** и воспользуйтесь командой **Создать/ Пакет** контекстного меню.

   В открывшемся окне укажите путь к сетевой папке общего доступа, содержащей дистрибутив Антивируса (см. п. 1). В диалоговом окне **Развертывание программы** выберите параметр **Назначенный** и нажмите на кнопку **ОК**.

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

3.4.2. Обновление версии приложения

Для обновления версии Антивируса Касперского:

1. Поместите дистрибутив, содержащий обновления Антивируса Касперского, в формате *.msi* в сетевую папку общего доступа.

2. Откройте **Редактор объектов групповой политики** и создайте новый пакет описанным выше способом.

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

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

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

3.4.3. Удаление приложения

Для удаления Антивируса Касперского:

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

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

   В диалоговом окне **Удаление приложений** выберите **Немедленное удаление этого приложения с компьютеров всех пользователей**, чтобы Антивирус Касперского был удален при следующей перезагрузке компьютера.

3.5. Обновление приложения с версии 5.0 до версии 6.0

Если у вас на компьютере установлено приложение Антивирус Касперского 5.0 для Windows Workstations, вы можете обновить его до Антивируса Касперского 6.0.

После запуска программы установки Антивируса Касперского 6.0 вам будет предложено сначала удалить установленную версию 5.0. По завершении удаления потребуется перезагрузка компьютера, после чего будет выполнена установка приложения версии 6.0.

Внимание!

При обновлении Антивируса Касперского версии 5.0 до 6.0 из сетевой папки, доступ к которой ограничен паролем, будет произведено удаление версии 5.0 и выполнена перезагрузка компьютера без последующей установки приложения версии 6.0. Это связано с отсутствие прав доступа к сетевой папке у программы установки. Для решения проблемы запускайте установку приложения только с локального ресурса.

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. 54);
- контекстное меню (см. п. 4.2 на стр. 55);
- главное окно (см. п. 4.3 на стр. 57);
- окно настройки параметров приложения (см. п. 4.4 на стр. 59).

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

- Microsoft Office Outlook: проверка на вирусы (см. п. 8.2.2 на стр. 113) и проверка на спам (см. п. 13.3.8 на стр. 198).
- Microsoft Outlook Express (Windows Mail) (см. п. 13.3.9 на стр. 201).
- The Bat!: проверка на вирусы (см. п. 8.2.3 на стр. 115) и проверка на спам (см. п. 13.3.10 на стр. 203).
- Microsoft Internet Explorer (см. Глава 11 на стр. 144).
- Microsoft Windows Explorer (см. п. 14.2 на стр. 206).

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 все компоненты защиты выключены (см. п. 2.2.1 на стр. 27).

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 сигнатур угроз и модулей 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. 55) и главному окну (см. п. 4.3 на стр. 57).

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.

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.

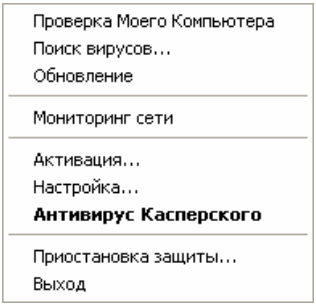


Рисунок 1. Контекстное меню

Обновление – запуск обновления модулей приложения и сигнатур угроз Антивируса Касперского и их установка на вашем компьютере.

Мониторинг сети – просмотр списка установленных сетевых соединений, открытых портов и трафика.

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 активировано.

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

Антивирус Касперского – открытие главного окна приложения (см. п. 4.3 на стр. 57).

Приостановка защиты / **Включение защиты** – выключение на время/включение работы компонентов защиты (см. п. 2.2.1 на стр. 27). Данный пункт меню не влияет на обновление приложения и на выполнение задач поиска вирусов.

Выход – завершение работы 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 две части:

- 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.

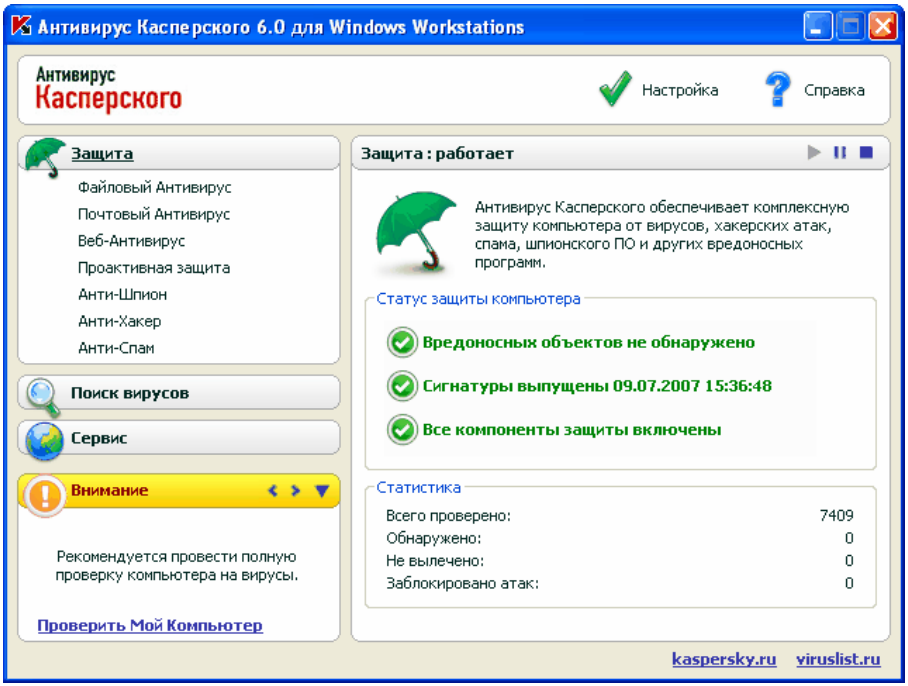
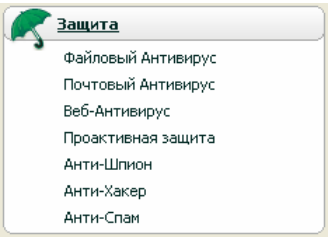
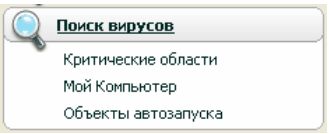
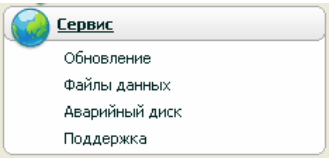
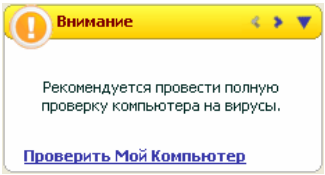


Рисунок 2. Главное окно Антивируса Касперского

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
Главная задача окна – информировать вас о статусе защиты вашего компьютера. Раздел **Защита** предназначен именно для этого. 	Чтобы просмотреть общую информацию о работе Антивируса Касперского, ознакомиться с общей статистикой работы приложения, убедиться, все ли компоненты корректно работают, выберите в навигационной части раздел **Защита**. Чтобы просмотреть параметры работы конкретного компонента защиты, достаточно в разделе **Защита** выбрать название компонента, по которому вы хотите получить информацию.
Для проверки компьютера на присутствие вредоносных объектов предусмотрен специальный раздел главного окна – **Поиск вирусов**. 	Данный раздел содержит список объектов, каждый из которых вы можете проверить на присутствие вирусов. Задачи, которые, по мнению экспертов «Лаборатории Касперского», вам понадобятся в первую очередь, сформированы и включены в раздел. Это задачи поиска вирусов в критических областях, среди объектов автозапуска, а также полная проверка компьютера.
Раздел **Сервис** включает дополнительные функции Антивируса Касперского. 	Здесь вы можете перейти к обновлению приложения, просмотреть отчеты о работе любого из компонентов Антивируса Касперского, перейти к работе с объектами на карантине, с резервными копиями, к информации о технической поддержке, к созданию диска аварийного восстановления системы и к окну управления лицензионными ключами.

Раздел навигационной части главного окна	Назначение
Раздел **комментариев и советов** сопровождает вашу работу с приложением. 	В этом разделе вы всегда сможете прочесть совет о том, как повысить степень защиты компьютера. Здесь же приводятся комментарии к текущей работе приложения и его параметрам. С помощью ссылок данного раздела вы можете сразу перейти к выполнению рекомендуемых в конкретном случае действий или более подробно ознакомиться с информацией.

Каждый элемент навигационной части сопровождается специальным контекстным меню. Так, для компонентов защиты и сервисных функций меню содержит пункты, позволяющие быстро перейти к их настройке, к управлению, к просмотру отчета. Для задач поиска вирусов и обновления 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.

4.4. Окно настройки параметров приложения

Окно настройки параметров Антивируса Касперского можно вызвать из главного окна (см. п. 4.3 на стр. 57). Для этого нажмите на ссылку Настройка в верхней его части.

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

- левая часть окна обеспечивает быстрый и удобный доступ к настройке каждого из компонентов приложения, 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.

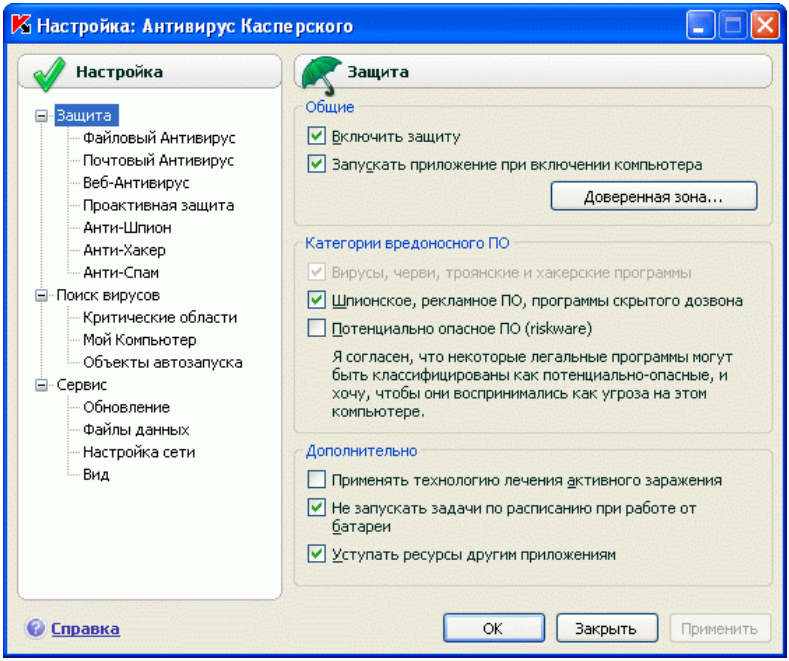


Рисунок 3. Окно настройки Антивируса Касперского

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. 40), 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, а также настроить работу Анти-Хакера, исходя из особенностей вашей сети.

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. 61).
- Провести обучение Анти-Спама в работе с вашими письмами (см. п. 5.5 на стр. 69).
- Обновить приложение, если это не было сделано с помощью мастера настройки либо автоматически сразу после установки приложения (см. п. 5.6 на стр. 71).
- Проверить компьютер на присутствие вирусов (см. п. 5.2 на стр. 67).

5.1. Каков статус защиты компьютера

Сводная информация о защите вашего компьютера представлена в главном окне Антивируса Касперского в разделе **Защита**. Здесь приведен текущий *статус защиты* компьютера и *общая статистика работы* приложения.

Статус защиты отражает текущее состояние защиты вашего компьютера с помощью специальных индикаторов (см. п. 5.1.1 на стр. 62). Статистика содержит итог текущей работы приложения (см. п. 5.1.2 на стр. 65).

5.1.1. Индикаторы защиты

Статус защиты определяется тремя индикаторами, которые отражают степень защиты вашего компьютера в данный момент времени и указывают на проблемы в настройке и работе приложения.

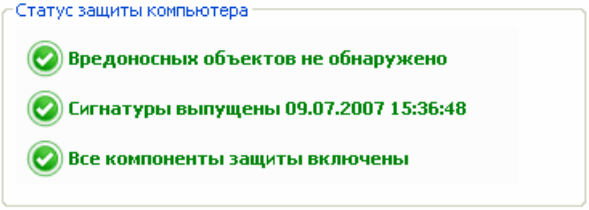


Рисунок 4. Индикаторы, отображающие статус защиты компьютера

Степень важности события, отображаемого индикатором, может иметь одно из следующих значений:

– *индикатор носит информационный характер*; указывает на то, что защита вашего компьютера на должном уровне, никаких проблем в настройке приложения и работе ее компонентов не наблюдается.

– *индикатор обращает ваше внимание на некоторые отклонения* в работе Антивируса Касперского от рекомендуемого режима работы, что может сказаться на защите информации. Пожалуйста, внимательно отнеситесь к рекомендациям специалистов «Лаборатории Касперского», приведенным в разделе комментариев и советов главного окна приложения.

– *индикатор отражает критически важные ситуации* в защите вашего компьютера. Пожалуйста, строго следуйте рекомендациям, приведенным в разделе комментариев и советов главного окна приложения. Все они направлены на повышение защиты вашего компьютера. Рекомендуемые действия оформлены в виде ссылок.

Рассмотрим подробнее индикаторы защиты и ситуации, на которые каждый из них указывает.

Первый индикатор отражает ситуацию с вредоносными объектами на вашем компьютере. Индикатор принимает одно из следующих значений:

Вредоносных объектов не обнаружено

Антивирус Касперского не обнаружил ни одного опасного объекта на вашем компьютере.

Все вредоносные объекты обезврежены

Антивирус Касперского вылечил все пораженные вирусами объекты и удалил те, что вылечить не удалось.

Обнаружены вредоносные объекты

В данный момент ваш компьютер подвержен риску заражения. Антивирус Касперского обнаружил вредоносные объекты, которые необходимо обезвредить. Для этого воспользуйтесь ссылкой Лечить все. По ссылке Подробнее вы можете получить детальную информацию о вредоносных объектах.

Второй индикатор отражает, насколько актуальна защита вашего компьютера на данный момент времени. Индикатор принимает одно из следующих значений:

Сигнатуры выпущены (дата, время)

Приложение не нуждается в обновлении. Все базы, используемые в работе Антивируса Касперского, содержат актуальную информацию по защите вашего компьютера.

Сигнатуры неактуальны

Модули приложения и сигнатуры угроз Антивируса Касперского не обновлялись несколько дней. Вы подвергаете ваш компьютер риску заражения новыми вредоносными программами или подвергнуться новым атакам, которые появились со дня последнего обновления приложения. Настоятельно рекомендуется обновить Антивирус Касперского. Для этого воспользуйтесь ссылкой Обновить.

Сигнатуры частично повреждены

Файлы сигнатур угроз частично повреждены. В данном случае рекомендуется еще раз запустить обновление приложения. Если при повторном обновлении ошибка не будет устранена, обратитесь в Службу технической поддержки «Лаборатории Касперского».

Необходимо перезагрузить компьютер

Для корректного обновления приложения требуется перезагрузка системы. Сохраните и закройте все файлы, с которыми вы работали, и воспользуйтесь ссылкой Перезагрузить компьютер.

Обновление приложения отключено

Сервис обновления сигнатур угроз и модулей приложения отключен. Для поддержания защиты в актуальном состоянии рекомендуется включить обновление.

Сигнатуры устарели

Антивирус Касперского не обновлялся очень давно. Вы подвергаете информацию на вашем компьютере большому риску. Обновите приложение как можно скорее. Для этого воспользуйтесь ссылкой Обновить.

Сигнатуры повреждены

Файлы сигнатур угроз полностью повреждены. В данном случае рекомендуется еще раз запустить обновление приложения. Если при повторном обновлении ошибка не будет устранена, обратитесь в Службу технической поддержки «Лаборатории Касперского».

Третий индикатор отражает, насколько полно используются возможности приложения. Индикатор принимает одно из следующих значений:

Все компоненты защиты включены

Антивирус Касперского защищает ваш компьютер на всех каналах проникновения вредоносных программ. Включены все компоненты защиты.

Защита не установлена

При инсталляции Антивируса Касперского не был установлен ни один из компонентов защиты. В данном режиме доступна только проверка объектов на вирусы. Для обеспечения максимальной защиты компьютера рекомендуется установить компоненты защиты.

Все компоненты защиты приостановлены

Работа всех компонентов защиты приостановлена на некото-

рое время. Чтобы возобновить работу компонентов выберите пункт **Включение защиты** в контекстном меню, открывающемся при нажатии по значку приложения в системной панели.

Некоторые компоненты защиты выключены

Отключен один или несколько компонентов защиты. Это может стать причиной заражения вашего компьютера и потери информации. Настоятельно рекомендуется включить защиту. Для этого выберите неактивный компонент в списке и нажмите на кнопку ▶.

Отключены все компоненты защиты

Защита компьютера полностью отключена, не работает ни один из ее компонентов. Чтобы возобновить работу компонентов выберите пункт **Включение защиты** в контекстном меню, открывающемся при нажатии по значку приложения в системной панели.

Некоторые компоненты защиты неисправны

Произошел сбой в работе одного или нескольких компонентов защиты Антивируса Касперского. В данной ситуации рекомендуется включить компонент или произвести перезагрузку компьютера (возможно требуется регистрация драйверов компонента после примененных обновлений).

5.1.2. Статус отдельного компонента Антивируса Касперского

Чтобы узнать, как Антивирус Касперского защищает файловую систему, почту, HTTP-трафик и другие источники проникновения опасных программ на ваш компьютер, как работают задачи поиска вирусов и как выполняется обновление сигнатур угроз, вам достаточно открыть соответствующий раздел главного окна приложения.

Например, для просмотра текущего статуса защиты файлов выберите раздел **Файловый Антивирус** в левой части главного окна приложения, а для просмотра статуса защиты от заражения новыми вирусами – раздел **Проактивная защита**. В правой части будет представлена сводная информация по работе компонента.

Для компонентов защиты она подразделяется на **статусную строку**, блок **Статус** (**Настройка** – для задач поиска вирусов и обновления) и блок **Статистика**.

Рассмотрим **статусную строку** компонента на примере Файлового Антивируса:

- *Файловый Антивирус : работает* – защита файлов обеспечивается на выбранном уровне (см. п. 7.1 на стр. 95).
- *Файловый Антивирус : пауза* – Файловый Антивирус выключен на некоторый промежуток времени. Компонент возобновит свою работу автоматически по истечении заданного периода или после перезагрузки приложения. Вы самостоятельно можете включить защиту файлов. Для этого нажмите на кнопку , расположенную в статусной строке.
- *Файловый Антивирус : выключено* – работа компонента остановлена пользователем. Вы можете включить защиту файлов. Для этого нажмите на кнопку , расположенную в статусной строке.
- *Файловый Антивирус : не работает* – защита файлов не доступна по каким-либо причинам.
- *Файловый Антивирус : 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».

Если в состав компонента входят несколько модулей, в разделе **Статус** приводится информация о статусах работы: включены ли они или выключены. Для тех компонентов, которые не имеют отдельных модулей, приводится собственный статус, уровень безопасности, который они обеспечивают, и для некоторых компонентов – действие над опасной программой.

Для задач поиска вирусов и обновления приложения блок **Статус** отсутствует. Уровень безопасности, применяемое к опасной программе действие для задач поиска вирусов, и режим запуска для обновления приводятся в блоке **Настройка**.

В блоке **Статистика** содержатся результаты работы компонента защиты, обновления или задачи поиска вирусов.

5.1.3. Статистика работы приложения

Статистика работы приложения приведена в блоке **Статистика** раздела **Защита** главного окна приложения (см. рис. 5) и показывает общую информацию о защите компьютера, зафиксированную с момента установки Антивируса Касперского.

Рисунок 5. Блок общей статистики работы приложения

Щелкнув левой клавишей мыши в любом месте блока, вы можете просмотреть отчет с детальной информацией. На соответствующих закладках приводится:

- информация о найденных объектах (см. п. 17.3.2 на стр. 250) и присвоенных им статусах;
- журнал событий (см. п. 17.3.3 на стр. 251);
- общая статистика проверки компьютера (см. п. 17.3.4 на стр. 252);
- параметры работы приложения (см. п. 17.3.5 на стр. 253).

5.2. 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 статистику последней проверки компьютера, параметры задачи: какой выбран уровень безопасности, какое действие будет применено к опасным объектам.

Чтобы проверить компьютер на присутствие вредоносных объектов,

1. Откройте главное окно приложения и выберите задачу **Мой компьютер** в разделе **Поиск вирусов**.
2. Нажмите на кнопку **Поиск вирусов**.

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

5.3. 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 статистику последней проверки данных областей, 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. Откройте главное окно приложения и выберите задачу **Критические области** в разделе **Поиск вирусов**.
2. Нажмите на кнопку **Поиск вирусов**.

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

5.4. 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. 6).

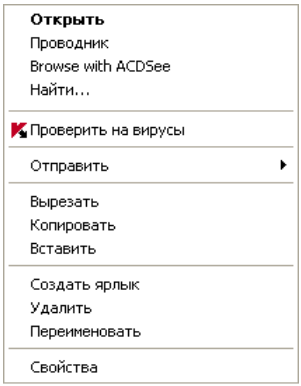


Рисунок 6. Проверка на присутствие вирусов объекта, выбранного средствами Microsoft Windows

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

5.5. Как обучить Анти-Спам

Одним из этапов подготовительной работы является обучение Анти-Спама работе с вашими письмами. Спам – это нежелательная корреспонденция, однако строго определить, что для отдельно взятого пользователя является спамом – очень сложно. Конечно, существуют категории писем, которые

можно с большой вероятностью отнести к спаму (например, письма массовой рассылки, реклама), однако для ряда пользователей такая корреспонденция также может быть полезной.

Поэтому мы предлагаем вам самостоятельно определить, какая почта является спамом, а какая – нет. Антивирус Касперского после установки предложит вам обучить компонент Анти-Спам различать спам и полезную почту. Сделать это вы можете с помощью специальных кнопок, встраиваемых в почтовый клиент (Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail), The Bat!), или посредством специального мастера обучения.

Внимание!

В данной версии Антивируса Касперского не предусмотрен модуль расширения Анти-Спама для Microsoft Office Outlook, установленного под Microsoft Windows 98.

Чтобы обучить Анти-Спам с помощью специальных кнопок,

1. Откройте почтовый клиент, используемый на вашем компьютере по умолчанию, например Microsoft Office Outlook. В панели инструментов вы увидите две кнопки: **Спам** и **Не спам**.
2. Выберите полезное письмо или группу писем, содержащую полезные письма, и нажмите на кнопку **Не спам**. С этого момента почтовые сообщения от отправителей выбранных вами писем всегда будут считаться полезной почтой.
3. Выберите письмо, содержащее ненужную вам информацию, группу писем или папку с такими письмами и нажмите на кнопку **Спам**. Анти-Спам проанализирует содержимое данных сообщений и в дальнейшем все письма схожего содержания с большой степенью вероятности будут считаться спамом.

Чтобы обучить Анти-Спам средствами специального мастера,

1. Откройте окно настройки приложения, выберите компонент Анти-Спам в разделе **Защита** и нажмите на кнопку **Мастер обучения**.
2. Следуйте указаниям Мастера обучения Анти-Спама (см. п. 13.2.1 на стр. 182).

В момент поступления письма в ваш почтовый ящик Анти-Спам проверит его на предмет спама и добавит специальные метки в заголовок **Тема** нежелательного почтового сообщения – [Spam]. Вы можете настроить в почтовом клиенте специальное правило для таких писем, например, правило удаления или помещения в специальную папку.

5.6. Как обновить приложение

«Лаборатория Касперского» обновляет сигнатуры угроз 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,

выберите компонент **Обновление** в разделе **Сервис** главного окна приложения и в правой части нажмите на кнопку **Обновить**.

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 19 на стр. 304).

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

Чтобы сохранить отчет в файл,

1. Выберите компонент в разделе **Защита** главного окна приложения и щелкните левой клавишей мыши в любом месте блока **Статистика**.
2. Нажмите на кнопку **Сохранить как** и в открывшемся окне укажите имя файла, в котором будут сохранены результаты работы компонента.

Чтобы сохранить отчет сразу всех компонентов Антивируса Касперского (компонентов защиты, задач поиска вирусов, сервисных функций),

1. Выберите раздел **Защита** в главном окне приложения и щелкните левой клавишей мыши в любом месте блока **Статистика**.

   или

   В окне отчета по любому компоненту воспользуйтесь ссылкой Все отчеты. В результате отчеты по всем компонентам приложения будут приведены на закладке **Отчеты**.
2. Нажмите на кнопку **Сохранить как** и в открывшемся окне укажите имя файла, в котором будут сохранены результаты работы приложения.

ГЛАВА 6. КОМПЛЕКСНОЕ УПРАВЛЕНИЕ ЗАЩИТОЙ

Антивирус Касперского предоставляет вам возможность комплексно управлять своей работой:

- Включать, отключать или приостанавливать работу приложения (см. п. 6.1 на стр. 73).
- Определять типы опасных программ, от которых Антивирус Касперского будет защищать ваш компьютер (см. п. 6.2 на стр. 78).
- Формировать список исключений из защиты (см. п. 6.3 на стр. 79).
- Создавать собственные задачи поиска вирусов и обновления (см. п. 6.4 на стр. 88).
- Настраивать запуск задач по удобному для вас расписанию (см. п. 6.5 на стр. 89).
- Настраивать параметры производительности (см. п. 6.6 на стр. 91) защиты компьютера.

6.1. Отключение / включение защиты вашего компьютера

По умолчанию Антивирус Касперского запускается при старте операционной системы, о чем вас информирует надпись *Антивирус Касперского 6.0* в правом верхнем углу экрана, и защищает ваш компьютер в течение всего сеанса работы. Все компоненты защиты (см. п. 2.2.1 на стр. 27) работают.

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

Внимание!

Специалисты «Лаборатории Касперского» настоятельно рекомендуют **не отключать 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 защиты означает отключение на некоторый промежуток времени всех ее компонентов, контролирующих файлы на вашем компьютере, входящую и исходящую почту, исполняемые скрипты, поведение приложений, а также Анти-Хакер и Анти-Спам.

Для того чтобы приостановить работу Антивируса Касперского,

1. В контекстном меню (см. п. 4.2 на стр. 55) приложения выберите пункт **Приостановка защиты**.
2. В открывшемся окне отключения защиты (см. рис. 7) 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. 6.1.5 на стр. 77).
   - **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.

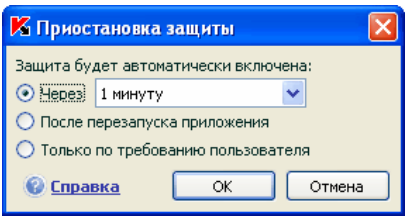


Рисунок 7. Окно приостановки защиты вашего компьютера

К вашему сведению.

Отключить защиту вашего компьютера можно одним из следующих способов:

- Нажмите на кнопку ⏸ в разделе **Защита**.
- В контекстном меню выберите пункт **Выход**. В данном случае приложение будет выгружена из оперативной памяти.

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

- Неактивные (серого цвета) названия выключенных компонентов в разделе **Защита** главного окна.
- Неактивный (серый) значок приложения в системной панели.
- Третий индикатор защиты (см. п. 5.1.1 на стр. 62) вашего компьютера, указывающий на то, что *Все компоненты защиты приостановлены*.

6.1.2. Полное отключение защиты компьютера

Полное отключение защиты означает остановку работы ее компонентов. Поиск вирусов и обновление продолжают работать в заданном 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. 6.3 на стр. 79).

Чтобы полностью отключить защиту компьютера,

1. Откройте окно настройки Антивируса Касперского 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.
- Третий индикатор защиты (см. п. 5.1.1 на стр. 62) вашего компьютера, указывающий на то, что *Отключены все компоненты защиты*.

6.1.3. Приостановка / отключение компонентов защиты или задач

Отключить работу какого-либо компонента защиты, задачи обновления или поиска вирусов 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. 6.3 на стр. 79).

Чтобы приостановить работу компонента защиты, выполнение задачи поиска вирусов или обновления,

выберите компонент или задачу в соответствующем разделе левой части главного окна приложения и нажмите на кнопку в статусной строке.

Статус компонента (задачи) изменится на *пауза*. Защита, обеспечиваемая компонентом, или выполняемая задача будет приостановлена до того момента, пока вы не возобновите их работу по кнопке .

Когда вы приостанавливаете работу компонента или задачи, статистика в текущем сеансе работы Антивируса Касперского сохраняется и будет продолжать формироваться после возобновления работы компонента или задачи.

Чтобы остановить работу компонента, поиск вирусов или обновление,

в статусной строке нажмите на кнопку . Остановить работу компонентов защиты можно также в окне настройки приложения, сняв флажок **Включить <имя_компонента>** в блоке **Общие** соответствующего компонента.

В этом случае статус компонента (задачи) поменяется на *выключено* (*прервано*). Защита, обеспечиваемая компонентом, или выполняемая задача будет остановлена до тех пор, пока вы не включите ее по кнопке . Для задач поиска вирусов и обновления вам будет предложено на выбор одно из действий: продолжить выполнение прерванной задачи или запустить ее заново.

При остановке компонента или задачи вся статистика предыдущей работы обнуляется и при запуске компонента будет формироваться заново.

6.1.4. Возобновление защиты вашего компьютера

Если в какой-либо момент времени вы приостановили или полностью отключили 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.

  Для этого нажмите на кнопку ▶ в статусной строке раздела **Защита** главного окна.

Статус защиты сразу же изменится на *работает*. Значок приложения в системной панели станет активным (цветным). Третий индикатор защиты (см. п. 5.1.1 на стр. 62) компьютера также уведомит, что *Все компоненты защиты включены.*

6.1.5. 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. 55) 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 Антивирус Касперского из меню **Пуск** → **Программы** → **Антивирус Касперского 6.0 для Windows Workstations** → **Антивирус Касперского 6.0 для Windows Workstations**.

Также защита может быть запущена автоматически после перезагрузки операционной системы. Чтобы включить этот режим в окне настройки приложения выберите раздел **Защита** и установите флажок ☑ **Запускать приложение при включении компьютера**.

6.2. Типы контролируемых вредоносных программ

Антивирус Касперского предлагает вам защиту от разных видов вредоносного программного обеспечения. Вне зависимости от установленных параметров приложение всегда защищает ваш компьютер от наиболее опасных видов вредоносных программ, какими являются 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, в окне настройки приложения (см. п. 4.4 на стр. 59) выберите раздел **Защита**.

Типы угроз (см. п. 1.1 на стр. 11) 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 обеспе-

чение, 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 сигнатур угроз 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 Касперского относит программу, которая, по вашему мнению, не является опасной, к категории потенциально опасных программ, рекомендуется настроить для нее исключение (см. п. 6.3 на стр. 79).

6.3. 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 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 именного этого объекта, правило исключения применено не будет.

Чтобы сформировать список исключений из защиты,

1. Откройте окно настройки приложения и выберите раздел **Защита**.
2. Нажмите на кнопку **Доверенная зона** в блоке **Общие**.
3. В открывшемся окне (см. рис. 8) настройте правила исключений для объектов, а также сформируйте список доверенных приложений.

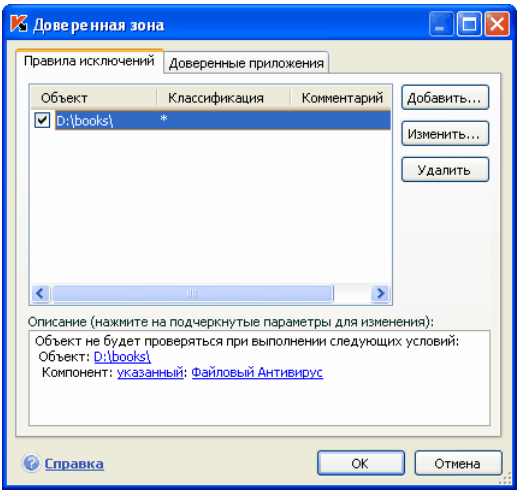


Рисунок 8. Формирование доверенной зоны

6.3.1. 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 классификации Вирусной энциклопедии.

Классификация – 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 исключающее правило, где в качестве классификации 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, Веб-Антивирус), 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** на закладке **Правила исключений**.
2. В открывшемся окне (см. рис. 9) выберите тип исключения в разделе **Параметры**:

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

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

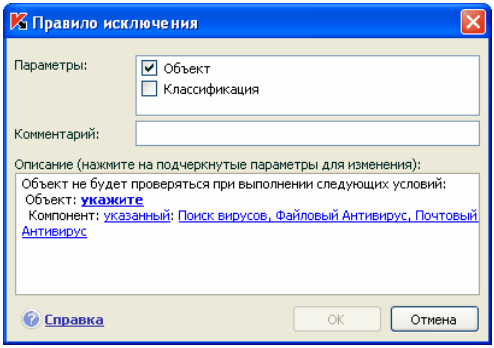


Рисунок 9. Создание правила исключения

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

- Если в качестве **Объекта** указан некоторый файл, а в качестве **Классификации** – 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 **Классификации** – 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. 333). 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 **Классификации** укажите полное имя исключаемой из проверки угрозы, как оно представлено в Вирусной энциклопедии, либо имя по маске (см. п. А.3 на стр. 334).

Для некоторых объектов по классификации 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, в следующих случаях:

- *Invader* (внедрение в процессы программ). Для данной угрозы 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 данной угрозы 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.kasperky.com* по ссылке из Microsoft Office Outlook. Для этого в качестве **Объекта** исключения укажите программу Microsoft Office Outlook, в качестве **Классификации** 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 исключающее правило.

Создание правила исключения из уведомления приложения об обнаружении опасного объекта:

1. В окне уведомления (см. рис. 10) 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**.

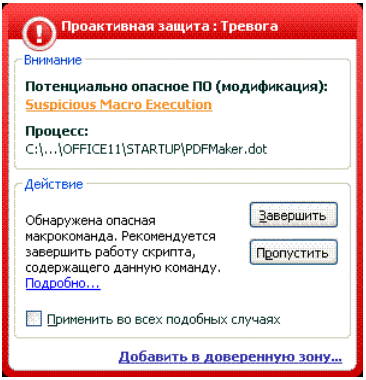


Рисунок 10. Уведомление об обнаружении опасного объекта

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. 11).

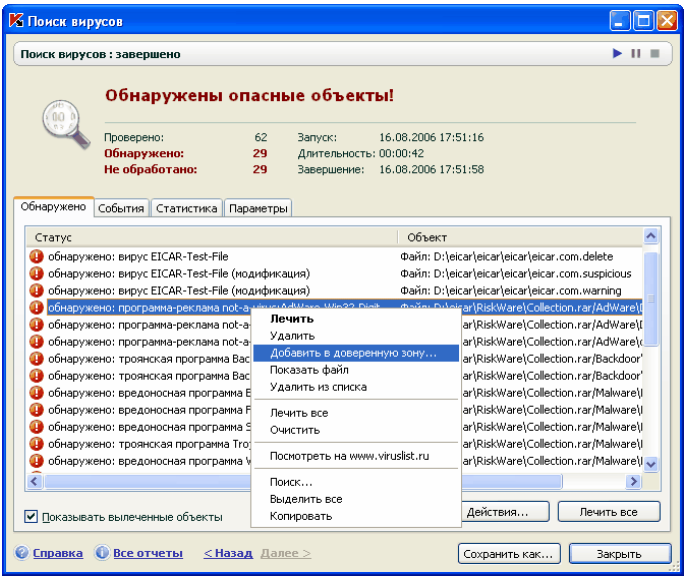


Рисунок 11. Создание правила исключения из отчета

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**.

6.3.2. Доверенные приложения

Исключение из проверки доверенных приложений доступно только в Антивирусе Касперского, установленном под управлением операционной системой Microsoft Windows NT 4.0/2000/XP/Vista.

Антивирус Касперского позволяет формировать список доверенных приложений, активность которых, в том числе и подозрительная, а также файловая, сетевая активность и обращения к системному реестру не будут контролироваться.

Например, вы считаете объекты, используемые стандартной программой Microsoft Windows – **Блокнот**, безопасными и не требующими проверки. Другими словами, вы доверяете этой программе. Чтобы исключить проверку объектов, используемых данным процессом, добавьте программу **Блокнот** в список доверенных 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. 6.3.1 на стр. 80).

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, создаваемый ими.

Формирование списка доверенных приложений осуществляется на специальной закладке **Доверенные приложения** (см. рис. 12). 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.

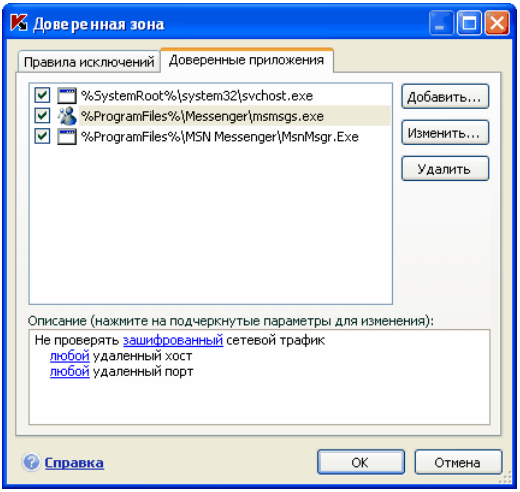


Рисунок 12. Список доверенных приложений

Для того чтобы добавить приложение в список доверенных:

1. Нажмите на кнопку **Добавить**, расположенную в правой части закладки **Доверенные приложения**.

2. В открывшемся окне **Доверенное приложение** (см. рис. 13) 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.

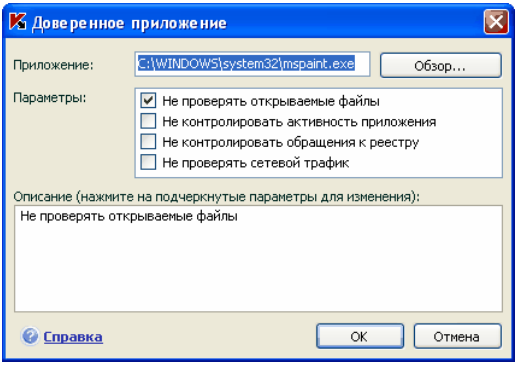


Рисунок 13. Добавление приложения в список доверенных

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.

> Обратите внимание, что при установленном флажке **Не проверять сетевой трафик** не проверяется трафик указанного приложения только на вирусы и спам. Однако это не влияет на проверку трафика компонентом Анти-Хакер, в соответствии с параметрами которого анализируется сетевая активность данного приложения.

6.4. Запуск задач с правами другого пользователя

В Антивирусе Касперского 6.0 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.

Обратите внимание, что данная возможность недоступна для операционной системы Microsoft Windows 98/ME.

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 от имени другой учетной записи,

1. Выберите имя задачи в разделе **Поиск вирусов** (для задач поиска вирусов) или **Сервис** (для задач обновления) главного окна и по ссылке Настройка перейдите в окно настройки параметров задачи.
2. Нажмите на кнопку **Настройка** в окне настройки задачи и в открывшемся окне перейдите на закладку **Дополнительно** (см. рис. 14).

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.

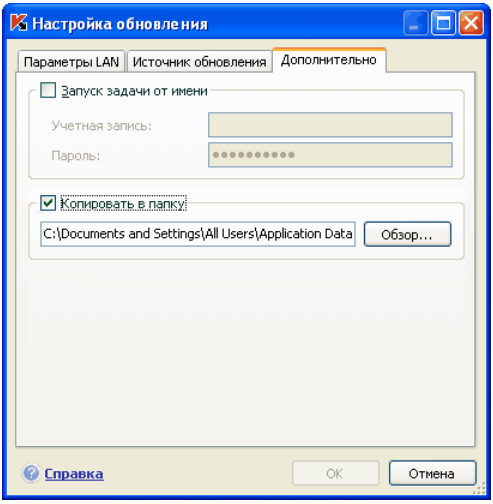


Рисунок 14. Настройка запуска задачи обновления от имени другой учетной записи

6.5. 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. Для этого в главном окне приложения в разделе **Поиск вирусов** (для задач поиска вирусов) или **Сервис** (для задачи обновления и копирования обновлений) выберите имя задачи и откройте окно ее настройки по ссылке Настройка.

Для того чтобы включить запуск задачи по расписанию, в блоке **Режим запуска** установите флажок с описанием условий автоматического запуска

задачи. Отредактировать условия запуска задачи проверки можно в окне **Расписание** (см. рис. 15), которое открывается по кнопке **Изменить**.

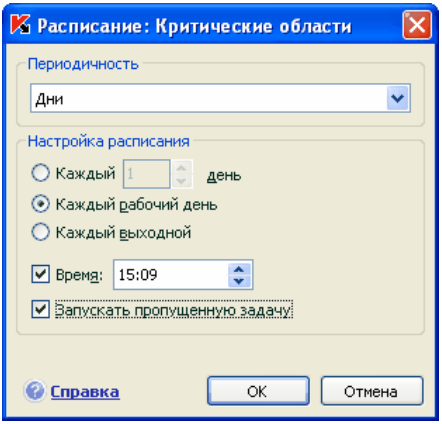


Рисунок 15. Формирование расписания запуска задач

Главное, что вам нужно определить, – это интервал, с которым должно выполняться событие (запуск задачи или отправка уведомления). Для этого выберите в блоке **Периодичность** (см. рис. 15) требующийся вариант. Далее необходимо указать параметры расписания для выбранного варианта в блоке **Настройка расписания**. На выбор предлагаются следующие варианты:

- **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.
- **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**.
- **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 вариант **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.

- **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**.
- **Месяцы**. Запуск задачи или отправка уведомлений выполняется один раз в месяц в указанное время.
- **В определенное время**. Производить запуск задачи или отправку уведомления в указанные день и время.
- **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.
- **После каждого обновления**. Задача запускается после каждого обновления сигнатур угроз (данный пункт относится только к задачам поиска вирусов).

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.

6.6. Настройка производительности

В целях экономии питания аккумулятора портативного компьютера, а также ограничения нагрузки на центральный процессор и дисковые подсистемы, 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. 71) или запустить проверку на вирусы (см. п. 5.2 на стр. 67). Чтобы воспользоваться сервисом экономии заряда аккумулятора, установите соответствующий флажок ☑ **Не запускать задачи по расписанию при работе от батареи**.
- 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, установите флажок **Уступать ресурсы другим приложениям**.

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.

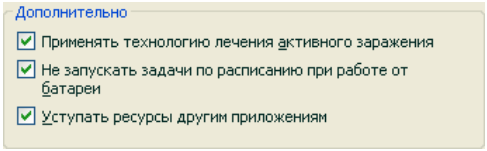


Рисунок 16. Настройка производительности

Чтобы настроить параметры производительности для задач поиска вирусов,

выберите раздел **Защита** главного окна приложения и воспользуйтесь ссылкой Настройка. Настройка параметров производительности производится в блоке **Дополнительно** (см. рис. 16).

6.7. Технология лечения активного заражения

Современные вредоносные программы могут внедряться на самые низкие уровни операционной системы, что делает процесс их удаления практически невозможным. Антивирус Касперского 6.0 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 использования процедуры расширенного лечения установите флажок **Применять технологию лечения активного заражения**.

Чтобы включить/ отключить использование технологии лечения активного заражения,

выберите раздел **Защита** главного окна приложения и воспользуйтесь ссылкой Настройка. Настройка параметров производительности производится в блоке **Дополнительно** (см. рис. 16).

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 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 *сигнатур угроз*, используемых в работе. Сигнатуры содержат описание всех известных на настоящий момент вредоносных программ, угроз, сетевых атак 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.

б. Если в файле обнаружен код, похожий на вредоносный, но стопроцентной гарантии этого нет, файл подвергается лечению и помещается в специальное хранилище – *карантин*.

в. 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):

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

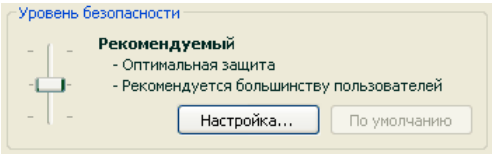


Рисунок 17. Уровни безопасности Файлового Антивируса

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 редактировать его параметры. В этом случае уровень станет **Пользовательским**. Рассмотрим пример, когда может пригодиться Пользовательский уровень безопасности файлов.

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 содержимому, 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,

нажмите на кнопку **Настройка** в окне настройки Файлового Антивируса, в открывшемся окне отредактируйте параметры защиты файлов и нажмите на кнопку **ОК**.

В результате будет сформирован четвертый уровень безопасности – **Пользовательский** – содержащий параметры защиты, заданные вами.

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. 97);
- параметры, формирующие защищаемую область (см. п. 7.2.2 на стр. 100);
- параметры, задающие действия над опасным объектом (см. п. 7.2.5 на стр. 104);
- дополнительные параметры работы Файлового Антивируса (см. п. 7.2.3 на стр. 102).

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 потенциально 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 становиться 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. 330), 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 выберите 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.

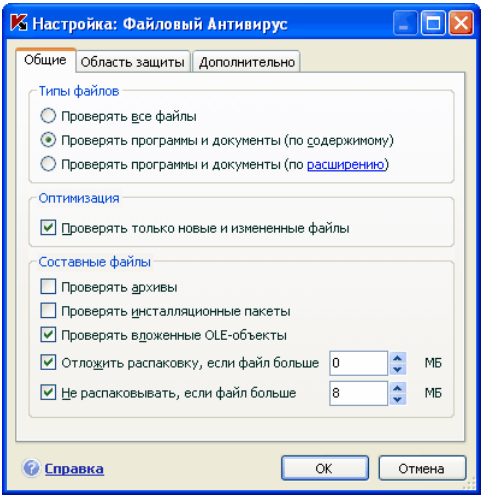


Рисунок 18. Выбор типов файлов, подвергаемых антивирусной проверке

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 инсталляционные 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 клавишей 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. Выберите **Файловый Антивирус** в главном окне и по ссылке Настройка перейдите в окно настройки компонента.
2. Нажмите на кнопку **Настройка** и в открывшемся окне выберите закладку **Область защиты** (см. рис. 19).

На закладке представлен список объектов, которые будет 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:

- Указать только те каталоги, диски или файлы, которые нужно защищать.
- Сформировать список объектов, которые защищать не нужно (см. п. 6.3 на стр. 79).
- Объединить первый и второй способы, то есть сформировать область защиты, из которой исключить ряд объектов.

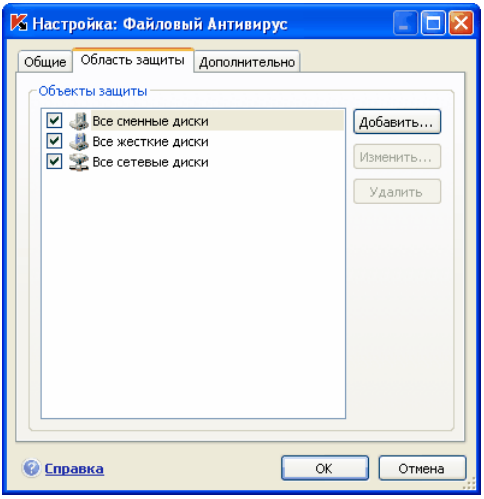


Рисунок 19. Формирование защищаемой области

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. Выберите **Файловый Антивирус** в главном окне и по ссылке Настройка перейдите в окно настройки компонента.
2. Нажмите на кнопку **Настройка** и в открывшемся окне выберите закладку **Дополнительно** (см. рис. 20).

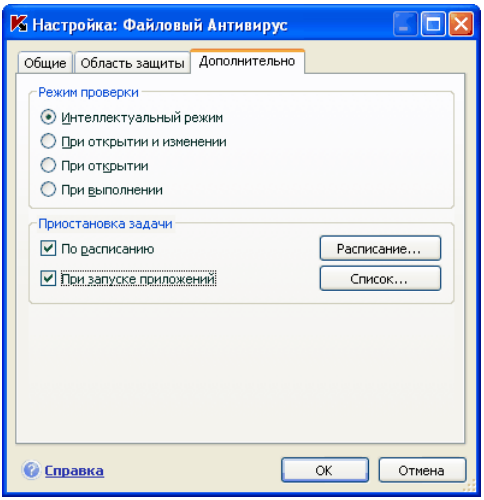


Рисунок 20. Настройка дополнительных параметров Файлового Антивируса

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.

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. 9), открывающемся по кнопке **Расписание** задайте временные рамки отключения и возобновления работы компонента. Для этого введите значения в формате ЧЧ:ММ в соответствующих полях.

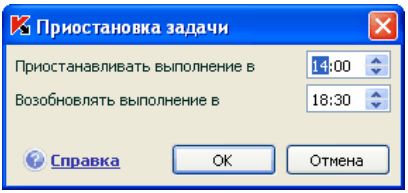


Рисунок 21. Приостановка работы компонента

Для отключения работы компонента при работе с программами, требующими значительных ресурсов, установите флажок ☑ **При запуске приложений** и в окне (см. рис. 22), открывающемся 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.

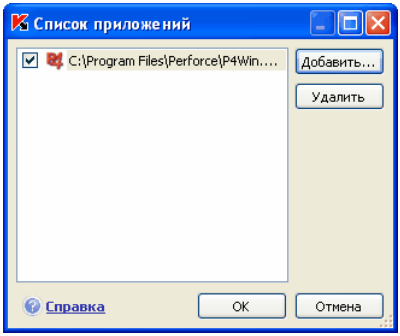


Рисунок 22. Формирование списка приложений

7.2.4. 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. Выберите **Файловый Антивирус** в главном окне и по ссылке Настройка перейдите в окно настройки компонента.
2. Нажмите на кнопку **По умолчанию** в разделе **Уровень безопасности**.

Если при настройке параметров Файлового Антивируса вы изменяли список объектов, включенных в область защиты, то при восстановлении первоначальных настроек вам будет предложено сохранить данный список для дальнейшего использования. Для сохранения списка объектов в открывшемся окне **Восстановление параметров** установите флажок **Область защиты**.

7.2.5. 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. 1.1 на стр. 11).
- *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,

выберите **Файловый Антивирус** в главном окне и по ссылке Настройка перейдите в окно настройки компонента. Все возможные действия приведены в соответствующем разделе (см. рис. 23).

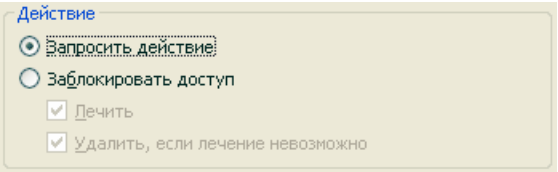


Рисунок 23. Возможные действия Файлового Антивируса над опасным объектом

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 предлагает на выбор одно из дальнейших действий. В зависимости от статуса объекта действия могут быть разными.
Заблокировать доступ	Файловый Антивирус блокирует доступ к объекту. Информация об этом фиксируется в отчете (см. п. 17.3 на стр. 246). Позже можно попытаться вылечить этот объект.

Если в качестве действия вы выбрали	При обнаружении опасного объекта
Заблокировать доступ **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 *возможно зараженный,* и он помещается на карантин (см. п. 17.1 на стр. 240). Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.
Заблокировать доступ **Лечить** **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. 17.2 на стр. 244).
Заблокировать доступ **Лечить** **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 **Файловый Антивирус** в главном окне приложения и щелкните левой клавишей мыши в любом месте блока **Статистика**.
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, MAPI[1] 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: заголовок 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 *сигнатур угроз*, используемых в работе приложения, и с помощью эвристического алгоритма. Сигнатуры содержат описание всех известных на настоящий момент вредоносных программ и способов их обезвреживания. Эвристический алгоритм позволяет обнаруживать новые вирусы, еще не описанные в сигнатурах угроз.
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. 113), 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. 115) 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 защиты почты

Антивирус Касперского обеспечивает защиту вашей почты на одном из следующих уровней (см. рис. 24):

Высокий – 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 при **Высоком** уровне, за исключением вложенных объектов или писем, проверка которых занимает больше трех минут.

Низкий – 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.

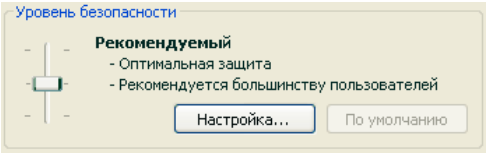


Рисунок 24. Выбор уровня безопасности почты

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. В этом случае уровень станет **Пользовательским**. Рассмотрим пример, когда может пригодиться Пользовательский уровень безопасности почты.

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 **Высокий** уровень 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,

нажмите на кнопку **Настройка** в окне настройки Почтового Антивируса, 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. 112);
- параметры проверки почтовых сообщений в Microsoft Office Outlook (см. п. 8.2.2 на стр. 113) и The Bat! (см. п. 8.2.3 на стр. 115).
- параметры, определяющие действия над опасными объектами почтовых сообщений (см. п. 8.2.4 на стр. 117).

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 безопасности, 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. Нажмите на кнопку **Настройка** в окне настройки Почтового Антивируса
2. В окне настройки Почтового Антивируса (см. рис. 25) выберите вариант **Только входящие сообщения** в блоке **Область защиты**.

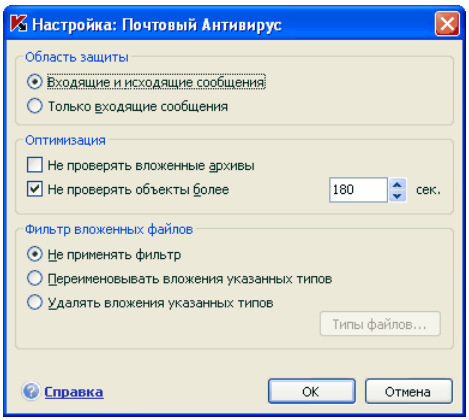


Рисунок 25. Настройка защиты почтового трафика

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.

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, открывающемся по кнопке **Типы файлов**.
- **Удалять вложения указанных типов** – отфильтровывать и удалять вложенные файлы определенного формата. Выбрать тип файла можно в окне, открывающемся по кнопке **Типы файлов**.

Подробнее о типах файлов вложений, подвергаемых фильтрации, вы можете прочесть в разделе А.1 на стр. 330.

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. 26).

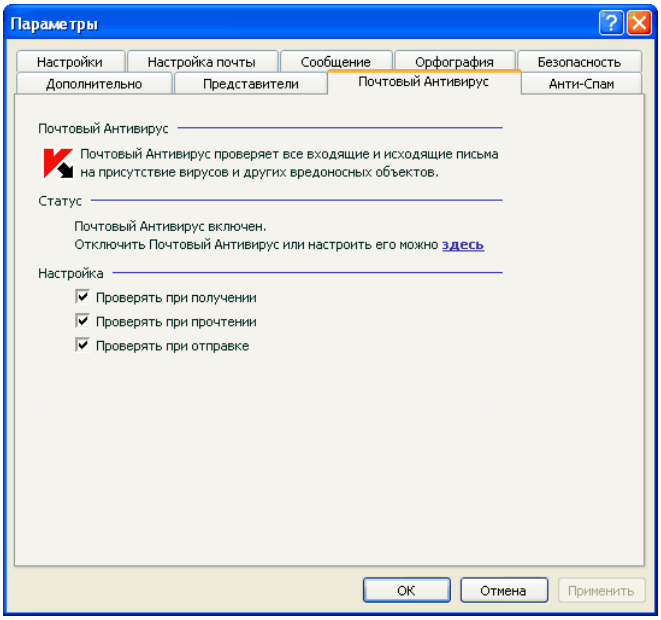


Рисунок 26. Детальная настройка защиты почты в Microsoft Office Outlook

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 самого приложения.

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. 112).

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. 27) распространяются на все установленные на компьютере антивирусные модули, поддерживающие работу с The Bat!

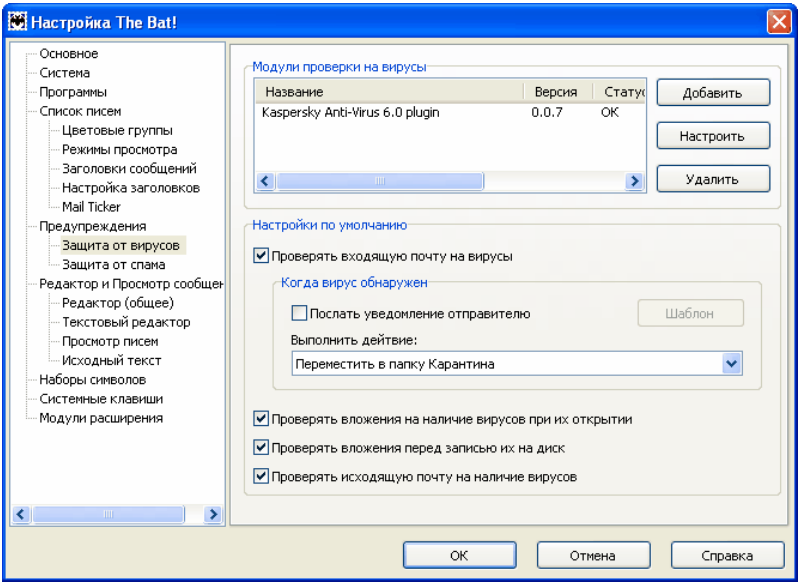


Рисунок 27. Настройка проверки почты в The Bat!

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 сообщении, 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. 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. Выберите **Почтовый Антивирус** в главном окне и по ссылке Настройка перейдите в окно настройки компонента.
2. Нажмите на кнопку **По умолчанию** в разделе **Уровень безопасности**.

8.2.5. 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 подозреваем 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. 1.1 на стр. 11);
- *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 Антивируса Касперского и выберите **Почтовый Антивирус**. Все возможные действия над опасными объектами приведены в блоке **Действие** (см. рис. 28).

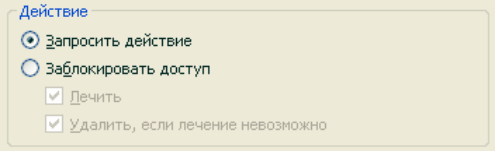


Рисунок 28. Выбор действия над опасным объектом письма

Рассмотрим подробнее возможные варианты обработки опасных объектов почтовых сообщений.

Если в качестве действия вы выбрали	При обнаружении опасного объекта
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.
Заблокировать доступ	Почтовый Антивирус блокирует доступ к объекту. Информация об этом фиксируется в отчете (см. п. 17.3 на стр. 246). Позже можно попытаться вылечить этот объект.
Заблокировать доступ **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 (см. п. 17.1 на стр. 240). Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.

Если в качестве действия вы выбрали	**При обнаружении опасного объекта**
◉ **Заблокировать доступ** ☑ **Лечить** ☑ **Удалить, если лечение невозможно**[2]	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 *возможно заражен* будет помещен на карантин.
◉ **Заблокировать доступ** ☐ **Лечить** ☑ **Удалить**	При обнаружении зараженного или возможно зараженного объекта Почтовый Антивирус удалит его без предварительного уведомления пользователя.

Перед лечением или удалением объекта Антивирус Касперского формирует его резервную копию и помещает ее в резервное хранилище (см. п. 17.2 на стр. 244) 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. 17.7 на стр. 266). 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, выходя в сеть с помощью модема, вам 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 приложение 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 *сигнатур угроз*, используемых в работе Антивируса Касперского, и с помощью эвристического алгоритма. Сигнатуры содержат описание всех известных на настоящий момент вредоносных программ и способов их обезвреживания. Эвристический алгоритм позволяет обнаруживать новые вирусы, еще не описанные в сигнатурах угроз.
2. В результате анализа возможны следующие варианты поведения:
    a. 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.
    б. 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.

Внимание!

Для перехвата и проверки http-трафика и скриптов на наличие вирусов требуется, чтобы Веб-Антивирус был запущен до момента установки соединения с веб-ресурсом. В противном случае проверка трафика осуществляться не будет.

9.1. Выбор уровня безопасности веб-защиты

Антивирус Касперского обеспечивает безопасность вашей работы в интернете на одном из следующих уровней (см. рис. 29):

Высокий – уровень, на котором осуществляется максимально полный контроль за скриптами и объектами, поступающими по HTTP-протоколу. Приложение детально проверяет все объекты, используя полный набор сигнатур угроз. 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 при **Высоком** уровне, однако ограничивают время кеширования фрагмента файла, что позволяет ускорить проверку и передачу объекта пользователю.

Низкий – 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 сигнатур угроз. Рекомендуется включать этот уровень безопасности, если на вашем компьютере установлены дополнительные средства веб-защиты.

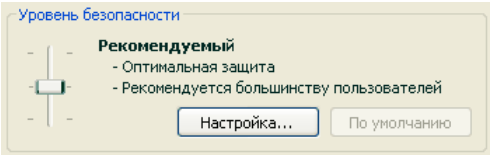


Рисунок 29. Выбор уровня веб-защиты

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 соответствует вашим требованиям, вы можете создать **Пользовательский** уровень безопасности. Рассмотрим пример, когда он может пригодиться.

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 (отсутствие централизованной веб-защиты и способ подключения к интернету).

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

Чтобы изменить параметры предустановленного уровня безопасности,

нажмите на кнопку **Настройка** в окне настройки Веб-Антивируса, в открывшемся окне отредактируйте параметры веб-защиты (см. п. 9.2 на стр. 123) 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 сигнатур угроз;
- сформировать список адресов, содержанию которых вы доверяете.

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 сигнатур угроз (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 сигнатур угроз, 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 таймаута на соединение HTTP-клиента.

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

1. Нажмите на кнопку **Настройка** в окне настройки Веб-Антивируса.
2. В открывшемся окне (см. рис. 30) выберите нужное значение в блоке **Алгоритм проверки**.

По умолчанию Веб-Антивирус проверяет данные из интернета с буферизацией, используя полный набор сигнатур угроз.

Внимание!

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

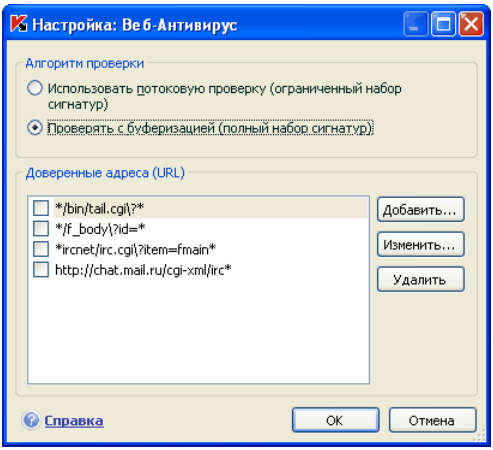


Рисунок 30. Настройка уровня веб-защиты

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. Нажмите на кнопку **Настройка** в окне настройки Веб-Антивируса.
2. В открывшемся окне (см. рис. 30) 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. 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. Выберите **Веб-Антивирус** в главном окне и по ссылке Настройка перейдите в окно настройки компонента.
2. Нажмите на кнопку **По умолчанию** в разделе **Уровень безопасности**.

9.2.4. 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 Антивируса Касперского и выберите **Веб-Антивирус**. Все возможные действия над опасными объектами приведены в блоке **Действие** (см. рис. 31).

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

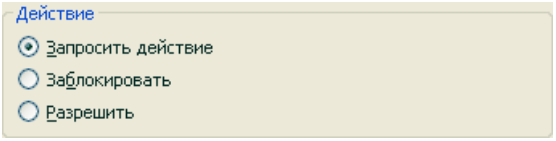


Рисунок 31. Выбор действия над опасным скриптом

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. 17.3 на стр. 246).
Разрешить	Веб-Антивирус разрешает доступ к опасному объекту. Информация об этом зафиксируется в отчете.

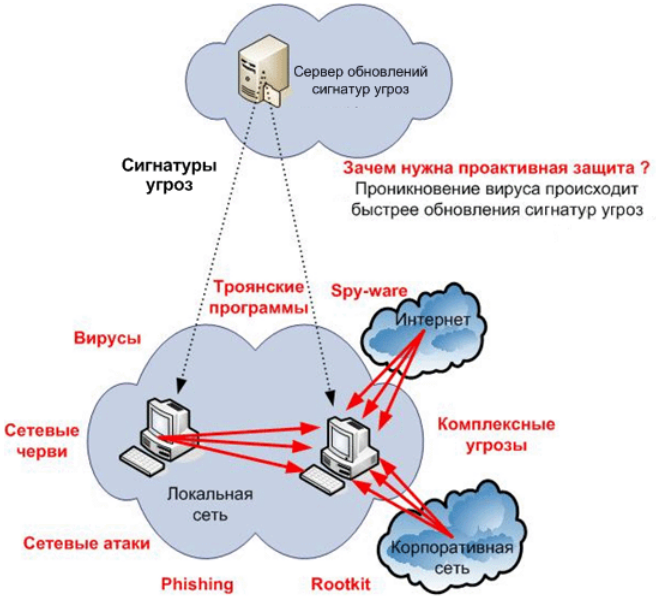
Что касается действий над опасными скриптами, то Веб-Антивирус всегда блокирует их исполнение и выводит на экран всплывающее сообщение, уведомляющее пользователя о выполненном действии. Вы не можете изменить действие над опасным скриптом, кроме как отключить работу модуля проверки скриптов.

ГЛАВА 10. ПРОАКТИВНАЯ ЗАЩИТА ВАШЕГО КОМПЬЮТЕРА

Внимание!

В данной версии приложения отсутствует компонент проактивной защиты **Проверка VBA-макросов** 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 сигнатур угроз. 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 мини-

мум одного фактического заражения новой угрозой, времени на анализ вредоносного кода, на добавление его в антивирусные базы и на обновление базы 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 сигнатур угроз, 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;
- скрытие процессов в системе;
- изменение определенных ключей системного реестра Microsoft Windows.

Все опасные операции отслеживаются и блокируются Проактивной защитой. Проактивная защита также отслеживает выполнение всех макросов, запускаемых в приложениях Microsoft Office.

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, макросов 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 приложения и обновляется вместе с сигнатурами угроз).

    - *Действия каждого запускаемого VBA-макроса* анализируются на предмет наличия признаков, характерных для вредоносной активности.

    - *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.

10.1. Настройка проактивной защиты

Проактивная защита осуществляется в строгом соответствии с параметрами (см. рис. 32), 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 каждой из которых вы можете настроить порядок обработки приложений (см. п. 10.1.1 на стр. 133) с такой активностью. Также предусмотрена возможность формирования исключений Проактивной защиты, где вы можете отменить контроль активности избранных приложений.

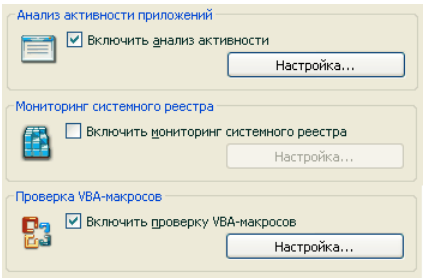


Рисунок 32. Параметры проактивной защиты

- 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 Microsoft Windows.

  Вы можете создать собственные правила (см. п. 10.1.3.2 на стр. 141) контроля в зависимости от ключа реестра Microsoft Windows.

- Выполняется ли проверка макросов.

  Контроль выполнения макросов на вашем компьютере регулируется флажком **Включить проверку VBA-макросов**. По умолчанию он установлен, а, следовательно, все действия макросов Visual Basic for Applications находятся под контролем Проактивной защиты.

  Вы можете выбрать, какие макросы считать опасными и что с ними делать (см. п. 10.1.2 на стр. 136).

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.

Вы можете настроить исключения (см. п. 6.3.1 на стр. 80) для модулей Проактивной защиты, а также сформировать список доверенных приложений (см. п. 6.3.2 на стр. 85).

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

10.1.1. 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. 6.3 на стр. 79), перечислив приложения, активность которых вы не считаете опасной.

Чтобы перейти к настройке контроля активности,

1. Откройте окно настройки Антивируса Касперского по ссылке Настройка из главного окна приложения.
2. Выберите компонент **Проактивная защита** в дереве настройки.
3. Нажмите на кнопку **Настройка** в блоке **Анализ активности приложений**.

Виды опасной активности, которые контролируются Проактивной защитой, приводятся в окне **Настройка: анализ активности** (см. рис. 33).

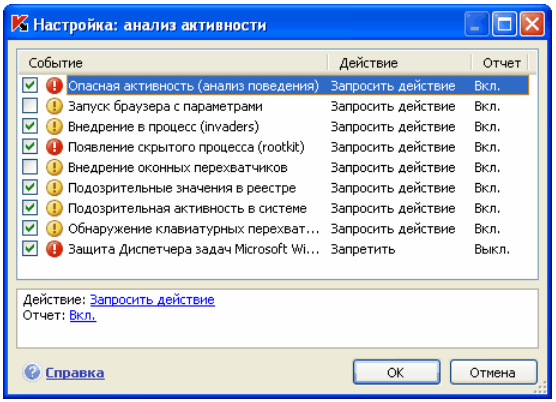


Рисунок 33. Настройка контроля активности приложений

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 запретить. Щелкайте левой клавишей мыши по ссылке с действием, пока она не примет нужное вам значение. Дополнительно к завершению процесса вы можете поместить 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. 34). По умолчанию данная возможность отключена.

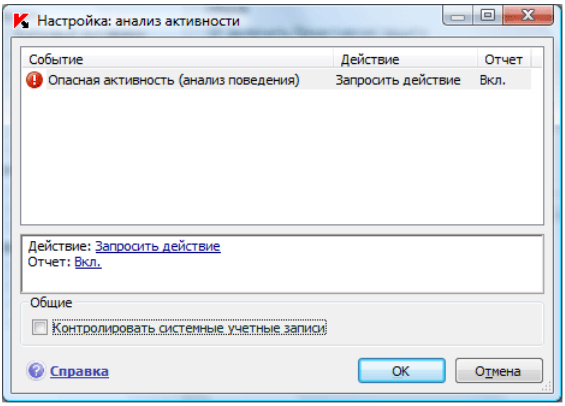


Рисунок 34. Настройка контроля активности приложений под Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64

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.

10.1.2. Контроль выполнения VBA-макросов

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.

Проверка и обработка опасных макросов, запускаемых на вашем компьютере, регулируется флажком **Включить проверку VBA-макросов**. По умолчанию флажок установлен, при этом активность каждого запускаемого макроса отслеживается на предмет опасного поведения, и, в случае обнаружения подозрительной активности, Проактивная защита разрешает или блокирует выполнение макроса.

Пример:

> Встраивание в приложение Microsoft Office Word панели Adobe Acrobat, позволяющей создать PDF-файл из любого документа, выполняется макросом *PDFMaker*. Такое действие, как встраивание элементов в программы, классифицируется Проактивной защитой как опасное. Если включен контроль VBA-макросов, при запуске макроса на экран будет выведено предупреждение от Проактивной защиты, уведомляющее вас о том, что обнаружена опасная макрокоманда. Вы можете выбрать, завершить работу данного макроса, прервав таким образом его выполнение, или разрешить.

Вы можете настроить, какие действия применять при выполнении макросом подозрительных действий. Если вы уверены, что выполнение макросом подозрительных действий при работе с конкретным объектом, например, документом Microsoft Word, не является опасным событием, рекомендуется сформировать правило исключения. При возникновении ситуации, отвечающей условиям правила исключения, подозрительное действие, выполняемое макросом, не будет обрабатываться Проактивной защитой.

Чтобы перейти к настройке проверки макросов,

1. Откройте окно настройки Антивируса Касперского по ссылке Настройка из главного окна приложения.
2. Выберите компонент **Проактивная защита** в дереве настройки.
3. Нажмите на кнопку **Настройка** в блоке **Проверка VBA-макросов**.

Настройка правил обработки опасных макросов ведется в окне **Настройка проверки VBA-макросов** (см. рис. 35). По умолчанию оно содержит правила для тех действий, которые классифицируются специалистами «Лаборатории Касперского» как опасные. К таким действиям, например, относится вставка модулей в программы, удаление файлов и т.д.

Если какое-либо из указанных в списке подозрительных действий вы не считаете опасным, снимите флажок рядом с его названием. Например, вы постоянно работаете с программой, которая выполняет макрос открытия некоторых файлов на запись, и вы совершенно уверены, что данная операция не является вредоносной.

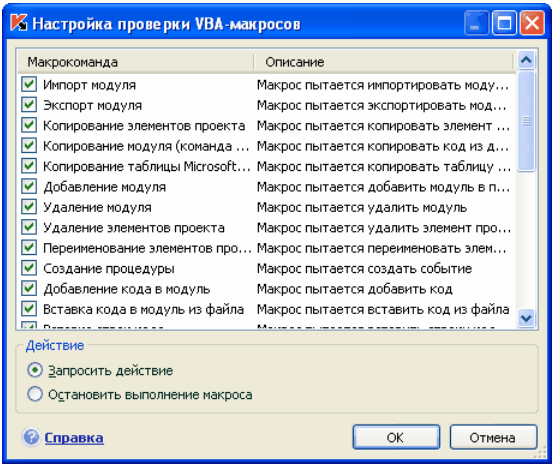


Рисунок 35. Настройка параметров проверки VBA-макросов

Чтобы Антивирус Касперского не блокировал выполнение макроса,

снимите флажок рядом с соответствующим действием. Более данное действие не будет считаться опасным и обрабатываться Проактивной защитой.

По умолчанию при обнаружении подозрительного действия, инициируемого макросом, приложение всегда выдает на экран запрос, разрешать или запрещать выполнение макроса.

Чтобы приложение автоматически блокировало выполнение всех опасных действий без предварительного запроса пользователя,

в окне со списком макросов назначьте в качестве обработки **Остановить выполнение макроса**.

10.1.3. 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 Антивируса Касперского по ссылке Настройка из главного окна приложения.
2. Выберите компонент **Проактивная защита** в дереве настройки.
3. Нажмите на кнопку **Настройка** в блоке **Мониторинг системного реестра**.

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. 36).

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 такому 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 для контроля ключей системного реестра в поле **Имя группы**.

2. Сформируйте список объектов системного реестра, которые будут входить в контролируемую группу, на закладке **Ключи** (см. п. 10.1.3.1 на стр. 140). Это может быть как один, так и несколько ключей.

3. Создайте правило для объектов реестра на закладке **Правила** (см. п. 10.1.3.2 на стр. 141). Вы можете создать несколько правил и определить приоритет их применения.

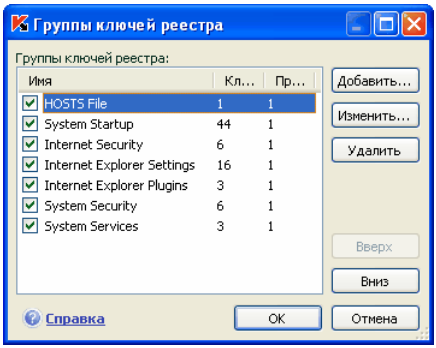


Рисунок 36. Контролируемые группы ключей системного реестра

10.1.3.1. 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 **Редактирование группы** (см. рис. 37).

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 правила объекта системного реестра.

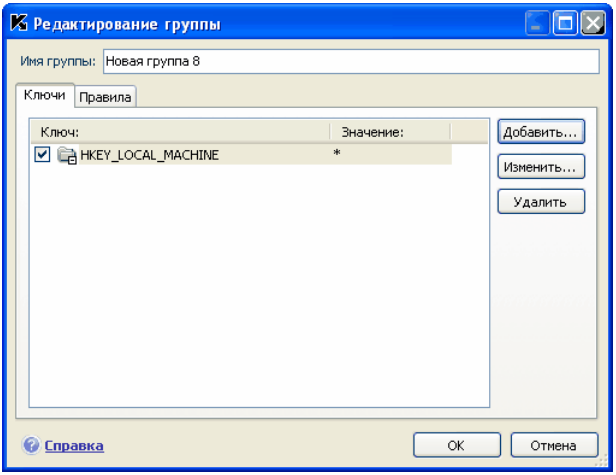


Рисунок 37. Добавление ключа реестра для контроля

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.

10.1.3.2. Создание правила для контроля объектов 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. 38).

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.

   - Укажите необходимость формирования отчета о выполненной операции. Для этого воспользуйтесь ссылкой протоколировать / не протоколировать.

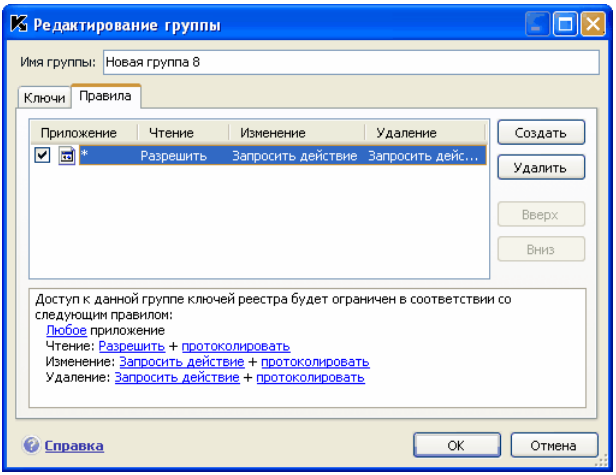


Рисунок 38. Создание правила контроля ключей системного реестра

Вы можете создать несколько правил и определить приоритет их выполнения с помощью кнопок **Вверх** и **Вниз**. Чем выше правило расположено в списке, тем выше его приоритет.

Разрешающее правило для объекта системного реестра также может быть создано из уведомления о попытке произвести операцию с объектом. Для этого в уведомлении воспользуйтесь ссылкой Создать разрешающее правило и в открывшемся окне укажите объект системного реестра, на который будет распространяться правило.

ГЛАВА 11. ЗАЩИТА ОТ РЕКЛАМЫ И ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Среди опасного программного обеспечения все большее распространение в последнее время получают программы, целью которых является:

- Кража вашей конфиденциальной информации (пароли, номера кредитных карт, важные документы и т.д.).
- Отслеживание ваших действий на компьютере, анализ установленного программного обеспечения.
- Навязчивая реклама различного содержания в окнах браузера, всплывающих окнах, в баннерах различных программ.
- Неавторизованный доступ в интернет с вашего компьютера на веб-сайты различного содержания.

На кражу информации нацелены фишинг-атаки и перехватчики клавиатуры, на трату ваших средств и времени – программы автоматического дозвона на платные веб-сайты, программы-шутки, программы-рекламы. Защита именно от таких программ и является задачей *Анти-Шпиона*.

В состав Анти-Шпиона входят следующие модули:

- *Анти-Фишинг* обеспечивает защиту от фишинг-атак.

  Фишинг-атаки, как правило, представляют собой почтовые сообщения от якобы финансовых структур, содержащие ссылки на их сайты. Текст сообщения убеждает воспользоваться ссылкой и ввести на открывшемся сайте конфиденциальную информацию, например, номер кредитной карты или свои имя и пароль персональной страницы интернет-банка, где можно производить финансовые операции.

  Частным примером фишинг-атаки является письмо от банка, клиентом которого вы являетесь, со ссылкой на официальный сайт в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его адрес в браузере, однако реально находитесь на фиктивном сайте. Все ваши дальнейшие действия на сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

  Ссылка на фишинг-сайт может быть вам направлена не только письмом, но и другими доступными для этого способами, например, в

тексте ICQ-сообщения. Анти-Фишинг отслеживает попытки открытия фишинг-сайта и блокирует его.

В состав сигнатур угроз Антивируса Касперского включены известные на настоящее время сайты, которые используются для фишинг-атак. Специалисты «Лаборатории Касперского» пополняют его адресами, предоставляемыми международной организацией по борьбе с фишингом (The Anti-Phishing Working Group). Данный список пополняется при обновлении сигнатур угроз.

- *Анти-Реклама* блокирует доступ к интернет-ресурсам с рекламной информацией, например, открытие всплывающих окон.

  Как правило, информация, размещенная во всплывающих окнах, не является полезной. Такие окна запускаются автоматически при открытии какого-либо сайта в интернете или переходе в другое окно по гиперссылкам. Они содержат рекламу и другую информацию, чтение которой вы никак не инициировали. Анти-Реклама блокирует открытие таких окон, о чем свидетельствует специальное сообщение над значком приложения в системной панели. Непосредственно в этом сообщении вы можете определить, хотите вы блокировать окно или нет.

  > Анти-Реклама корректно работает с модулем, блокирующим всплывающие окна в Microsoft Internet Explorer, входящим в состав пакета обновлений Service Pack 2 для Microsoft Windows XP. При установке приложения в браузер встраивается модуль расширения, который позволяет разрешить открытие всплывающего окна непосредственно в браузере.

  На некоторых сайтах всплывающие окна используются для организации более удобного и быстрого доступа к информации. Если вы часто работаете с такими сайтами, и информация, содержащаяся во всплывающих окнах, крайне важна для вас, рекомендуем вам добавить их в список доверенных сайтов (см. п. 11.1.1 на стр. 147). Всплывающие окна на доверенных сайтах не будут блокироваться.

  При работе с Microsoft Internet Explorer блокирование всплывающего окна сопровождается значком в статусной строке браузера. По нажатию на него вы можете снять блокировку либо добавить адрес в список доверенных адресов.

- *Анти-Баннер* блокирует рекламную информацию, размещенную на специальных баннерах в интернете или встроенных в интерфейс различных программ, установленных на вашем компьютере.

  Рекламная информация на баннерах не только не содержит полезной информации, но и отвлекает вас от дел и повышает объем скачиваемого трафика. Анти-Баннер блокирует самые распространен-

ные на настоящее время баннеры, маски которых включены в поставку Антивируса Касперского. Вы можете отключить блокировку баннеров либо сформировать собственные списки разрешенных и запрещенных баннеров.

Для интеграции модуля Анти-Баннер с браузером **Opera** добавьте в файл *standard_menu.ini*, раздел **[Image Link Popup Menu]** следующую строку:

Item, «New banner» = Copy image address & Execute program, «<диск>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Workstations\opera_banner_deny.vbs», «//nologo %C»

- *Анти-Дозвон* обеспечивает защиту от попыток несанкционированного модемного соединения.

Анти-Дозвон работает на операционных системах Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows XP x64, Microsoft Windows Vista и Microsoft Windows Vista x64.

Как правило, программы несанкционированного дозвона устанавливают соединение с определенными веб-сайтами, например, порнографического характера. В результате вы вынуждены оплачивать дорогостоящий трафик, получение которого вами инициировано не было. Если вы хотите исключить какой-либо номер из блокируемого списка, вам нужно включить его в список доверенных номеров (см. п. 11.1.3 на стр. 151).

11.1. Настройка Анти-Шпиона

Защита от интернет-мошенничества и навязчивой рекламы обеспечивается с учетом всех известных специалистам «Лаборатории Касперского» программ, которые могут привести к краже конфиденциальной информации и трате ваших денежных средств. Вы можете провести более детальную настройку компонента, а именно:

- Создать список доверенных адресов веб-сайтов (см. п. 11.1.1 на стр. 147), всплывающие окна которых не будут блокироваться.
- Сформировать «белый» и «черный» списки баннеров (см. п. 11.1.2 на стр. 148).
- Сформировать набор доверенных телефонных номеров (см. п. 11.1.3 на стр. 151), Dial-up-соединение по которым вы разрешаете.

11.1.1. Формирование списка доверенных адресов Анти-Рекламы

По умолчанию модуль Анти-Реклама блокирует большинство всплывающих окон, которые открываются автоматически, без вашего запроса. Исключением являются всплывающие окна веб-сайтов, включенных в список доверенных в Microsoft Internet Explorer, и сайтов внутренней сети (интранет), в которой вы зарегистрированы в данный момент.

Если на вашем компьютере установлена операционная система Microsoft Windows XP с пакетом обновлений Service Pack 2, то в составе Microsoft Internet Explorer входит собственный блокиратор всплывающих окон. Вы можете настраивать его работу, выбирая, какие именно окна вы хотели бы блокировать, а какие – нет. Анти-Реклама поддерживает совместную работу с этим блокиратором по следующему принципу: при попытке открытия всплывающего окна всегда будет превалировать запрещающее правило. Например, адрес некоторого всплывающего окна добавлен в список разрешенных окон Microsoft Internet Explorer, но не входит в доверенные адреса Анти-Рекламы, то такое окно будет заблокировано. И напротив, если в браузере выбрано условие блокирования всех всплывающих окон, то даже если адрес окна включен в список доверенных адресов Анти-Рекламы, оно все равно будет заблокировано. Именно поэтому рекомендуется при работе с Microsoft Windows XP Service Pack 2 производить совместную настройку браузера и Анти-Рекламы.

Если какие-либо окна вы хотели бы просматривать по тем или иным причинам, нужно добавить их в список доверенных адресов. Для этого:

1. Откройте окно настройки Антивируса Касперского и выберите Анти-Шпион в дереве настройки.
2. Нажмите на кнопку **Доверенные адреса** в разделе блокирования всплывающих окон.
3. В открывшемся окне (см. рис. 39) нажмите на кнопку **Добавить** и укажите маску сайтов, всплывающие окна которых блокировать не нужно.

   К вашему сведению.

   При вводе маски доверенного адреса можно использовать символы * и ?.

   Например, маска http://www.test* исключает всплывающие окна любых сайтов, начинающихся с указанной последовательности.

4. Укажите, будут ли исключаться из проверки адреса, входящие в доверенную зону Microsoft Internet Explorer или являющиеся адре-

сами вашей локальной сети. По умолчанию приложение считает их доверенными и не блокирует всплывающие окна данных адресов.

Новое исключение будет добавлено в начало списка доверенных адресов. Для того чтобы отказаться от использования добавленного вами исключения, вам достаточно просто снять флажок рядом с его именем. Если вы хотите совсем отказаться от какого-либо исключения, выберите его в списке и воспользуйтесь кнопкой **Удалить**.

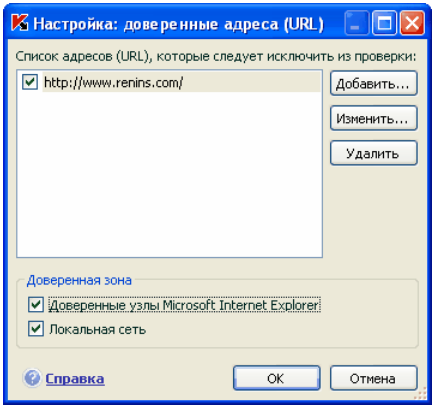


Рисунок 39. Формирование списка доверенных адресов

Если вы хотите блокировать всплывающие окна интранета и веб-сайтов, включенных в список доверенных для Microsoft Internet Explorer, снимите соответствующие флажки в разделе **Доверенная зона**.

При открытии всплывающих окон, не входящих в список доверенных, над значком приложения всплывает уведомление, сообщающее о блокировании окна. Посредством ссылок этого уведомления вы можете отказаться от блокирования и добавить адрес окна в список доверенных.

Аналогичные действия вы можете выполнить и при работе в Microsoft Internet Explorer, входящем в состав Microsoft Windows XP с пакетом обновлений Service Pack 2. Для этого воспользуйтесь контекстным меню, которое вы можете открыть на значке приложения, появляющемся в нижней части окна браузера при блокировании всплывающих окон.

11.1.2. Списки адресов блокируемых баннеров

Список масок наиболее распространенных рекламных баннеров составлен специалистами «Лаборатории Касперского» на основании специально про-

веденного исследования и включен в поставку приложения. Рекламные баннеры, подпадающие под маски этого списка, будут блокироваться приложением, если блокировка баннеров не отключена.

Кроме того, вы можете создать «белый» и «черный» списки баннеров, на основании которых трансляция баннера будет разрешена или запрещена.

Обратите внимание, что при наличии маски домена в списке запрещенных баннеров или «черном» списке доступ к корню сайта не блокируется.

Например, если в список запрещенных баннеров внесена маска **truehits.net**, то доступ к сайту **http://truehits.net** будет разрешен, а доступ к **http://truehits.net/a.jpg** – заблокирован.

11.1.2.1. Настройка стандартного списка блокируемых баннеров

В поставку Антивируса Касперского включен список масок самых распространенных баннеров, запускаемых на веб-сайтах в интернете и в интерфейсах различных программ. Этот список составлен специалистами «Лаборатории Касперского» и обновляется вместе с сигнатурами угроз.

Вы можете выбрать, какие стандартные маски баннеров вы хотите использовать при работе Анти-Баннера. Для этого:

1. Откройте окно настройки Антивируса Касперского и выберите Анти-Шпион в дереве настройки.
2. Нажмите на кнопку **Настройка** в разделе блокирования рекламных баннеров.
3. Откройте закладку **Общие** (см. рис. 40). Приведенные на закладке маски баннеров блокируются Анти-Баннером. Строка маски может быть использована в любом месте адреса баннера.

Список стандартных блокируемых масок не доступен для редактирования. Если вы не хотите блокировать баннер, соответствующий какой-либо стандартной маске, вам нужно снять флажок ☑ рядом с маской.

Для анализа баннеров, не подпадающих под маски стандартного списка, установите флажок ☑ **Использовать методы эвристического анализа**. В данном случае приложение будет анализировать загружаемые изображения на предмет наличия признаков, характерных для баннеров. На основании этого анализа изображение может быть идентифицировано как баннер и заблокировано.

Кроме того, вы можете сформировать собственные списки разрешенных или запрещенных для трансляции баннеров. Это можно сделать на закладках **«Белый» список** и **«Черный» список**.

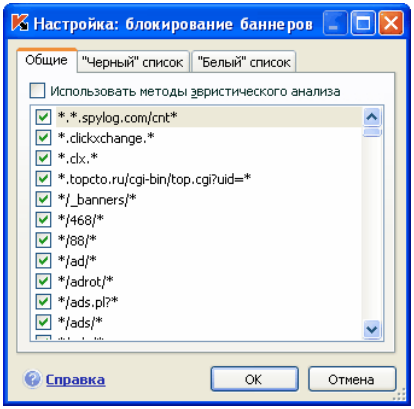


Рисунок 40. Список блокируемых баннеров

11.1.2.2. «Белый» список баннеров

«Белый» список баннеров формируется пользователем в процессе работы с приложением, если возникает необходимость не блокировать некоторые баннеры. Этот список содержит маски разрешенных к трансляции баннеров.

Чтобы добавить новую маску в «белый» список:

1. Откройте окно настройки Антивируса Касперского и выберите Анти-Шпион в дереве настройки.
2. Нажмите на кнопку **Настройка** в разделе блокирования рекламных баннеров.
3. Откройте закладку **«Белый» список**.

По кнопке **Добавить** внесите в список маску разрешенного баннера. Вы можете указать полный адрес (URL) баннера или его маску. В последнем случае при попытке открытия баннера в его адресе будет производиться поиск указанной маски.

При вводе маски баннера можно использовать символы ***** и **?** (где * – любая последовательность символов, а ? – любой один символ).

Чтобы отказаться от использования какой-либо введенной вами маски, вам необязательно удалять ее из списка, достаточно снять флажок ☑ рядом с

ней. В данном случае баннеры, подходящие под эту маску, не будут считаться исключением.

С помощью кнопок **Импорт** и **Экспорт** вы можете копировать сформированные списки разрешенных баннеров с одного компьютера на другой.

11.1.2.3. «Черный» список баннеров

Дополнительно к списку стандартных масок баннеров (см. п. 11.1.2.1 на стр. 149), блокируемых Анти-Баннером, вы можете составить собственный список. Для этого:

1. Откройте окно настройки Антивируса Касперского и выберите Анти-Шпион в дереве настройки.
2. Нажмите на кнопку **Настройка** в разделе блокирования рекламных баннеров.
3. Откройте закладку **«Черный» список**.

По кнопке **Добавить** внесите в список маску того баннера, который вы хотели бы блокировать Анти-Баннером. Вы можете указать полный адрес (URL) баннера или его маску. В последнем случае при попытке открытия баннера в его адресе будет производиться поиск указанной маски.

При вводе маски баннера можно использовать символы ***** и **?** (где * – любая последовательность символов, а ? – любой один символ).

Чтобы отказаться от использования какой-либо введенной вами маски, вам необязательно удалять ее из списка, достаточно снять флажок ☑ рядом с ней.

С помощью кнопок **Импорт** и **Экспорт** вы можете копировать сформированные списки блокируемых баннеров с одного компьютера на другой.

11.1.3. Формирование списка доверенных номеров Анти-Дозвона

Модуль Анти-Дозвон контролирует номера телефонов, по которым выполняется скрытое соединение с интернетом. Скрытым считается соединение, в параметрах которого задано не уведомлять пользователя о соединении, а также соединение, не инициируемое вами.

Каждый раз, когда выполняется попытка скрытого соединения, на экран выводится специальное уведомление, сообщающее вам об этом. В данном уведомлении вам нужно определить, разрешить или запретить его. Если вы

не инициировали такого соединения, высока вероятность, что это действие вредоносной программы.

Если вы хотите разрешать соединения по каким-либо номерам без предварительного запроса приложения, вам нужно добавить их в список доверенных номеров. Для этого:

1. Откройте окно настройки Антивируса Касперского и выберите Анти-Шпион в дереве настройки.
2. Нажмите на кнопку **Доверенные номера** в разделе блокирования автодозвона на сайты.
3. В открывшемся окне (см. рис. 41) нажмите на кнопку **Добавить** и укажите номер или маску номера, соединение по которому блокировать не нужно.

К вашему сведению.

При вводе маски доверенного номера можно использовать символы * и ?.

Например, маска *8???79787** будет распространяться на любые номера, начинающиеся с цифр *79787*, где код города состоит из любых трех цифр.

Новое исключение будет добавлено в начало списка доверенных номеров. Для того чтобы отказаться от использования добавленного вами номера как исключения, вам достаточно просто снять флажок ☑ рядом с ним в списке. Если вы хотите совсем отказаться от какого-либо исключения, выберите его в списке и нажмите на кнопку **Удалить**.

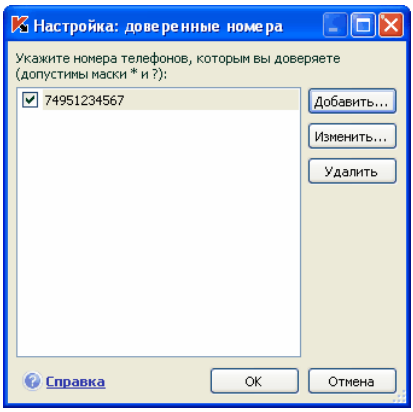
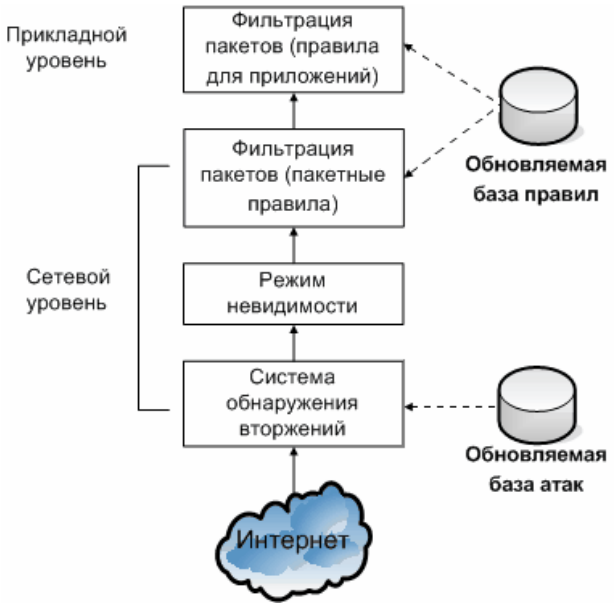


Рисунок 41. Формирование списка доверенных адресов

ГЛАВА 12. ЗАЩИТА ОТ СЕТЕВЫХ АТАК

В настоящее время компьютер стал достаточно уязвим при работе в интернете. Он подвержен не только заражению вирусами, но и различного рода атакам, использующим уязвимости операционных систем и программного обеспечения.

Для обеспечения безопасности вашей работы в локальных сетях и интернете предназначен специальный компонент Антивируса Касперского – *Анти-Хакер*. Он защищает ваш компьютер на сетевом и прикладном уровнях, а также обеспечивает невидимость компьютера в сети для предотвращения атак. Рассмотрим подробнее, на чем построена работа Анти-Хакера.



Защита на сетевом уровне обеспечивается за счет использования глобальных правил для сетевых пакетов, где на основании анализа таких параметров, как направление движения пакета, протокол передачи пакета, порт назначения или выхода пакета, разрешается или блокируется сетевая активность. Правила для пакетов определяют сетевую доступность независимо от установленных на вашем компьютере приложений, использующих сеть.

В дополнение к правилам для пакетов защита на сетевом уровне обеспечивается *подсистемой обнаружения вторжений* (IDS). Задача этой подсистемы заключается в анализе входящих соединений, определении факта сканирования портов вашего компьютера, а также фильтрации сетевых пакетов, направленных на использование уязвимостей программного обеспечения. При срабатывании подсистемы обнаружения вторжений все входящие соединения с атаковавшего компьютера блокируются на определенное время, а пользователь получает уведомление о том, что его компьютер подвергся сетевой атаке.

Работа подсистемы обнаружения вторжений основана на использовании в ходе анализа специальной сигнатурной базы атак (см. п. 12.9 на стр. 172), которая регулярно пополняется специалистами «Лаборатории Касперского» и обновляется вместе с сигнатурами угроз.

Защита на прикладном уровне обеспечивается за счет применения правил использования сетевых ресурсов приложениями, установленными на вашем компьютере. Как и защита на сетевом уровне, защита на прикладном уровне строится на анализе сетевых пакетов с учетом направления движения пакета, типа протокола его передачи, а также используемого порта. Однако на прикладном уровне учитываются не только характеристики сетевого пакета, но и конкретное приложение, которому адресован данный пакет либо которое инициировало отправку этого пакета.

Использование правил для приложений дает возможность более тонкой настройки защиты, когда, например, определенный тип соединения запрещен для одних приложений, но разрешен для других.

Исходя из двух уровней защиты Анти-Хакера существуют два типа правил:

- *Правила для пакетов* (см. п. 12.3 на стр. 161). Используются для ввода общих ограничений сетевой активности независимо от установленных приложений. Пример: при создании пакетного правила, запрещающего входящие соединения на порт 21, ни одно приложение, использующее этот порт (например, ftp-сервер), не будет доступно извне.
- *Правила для приложений* (см. п. 12.2 на стр. 157). Используются для ввода ограничений сетевой активности конкретного приложения. Пример: если запрещено соединение по порту 80 для каждого из приложений, вы можете создать правило, разрешающее соединения с использованием этого порта, только для веб-браузера FireFox.

Правила для сетевых пакетов и правила для приложений могут быть *разрешающие* и *запрещающие*. В поставку приложения включен набор правил, регламентирующих сетевую активность наиболее распространенных приложений, а также работу компьютера с распространенными протоколами и портами. Кроме того в дистрибутив Антивируса Касперского включен набор разрешающих правил для доверенных приложений, сетевая активность которых не вызывает сомнений.

Для упрощения настройки и применения правил в Антивирусе Касперского существует разделение всего сетевого пространства на *зоны безопасности*, зачастую совпадающие с подсетями, в которые включен компьютер. Каждой из зон вы можете присвоить статус (*Интернет, Локальная сеть, Доверенная*), на основании которого будет определена политика применения правил и контроля сетевой активности в данной зоне (см. п. 12.5 на стр. 166).

Специальный режим работы Анти-Хакера – *режим невидимости* – предотвращает обнаружение компьютера извне. В результате хакеры теряют объект для атаки. В то же время на вашу работу в интернете режим не оказывает никакого влияния (при условии, что компьютер не используется в качестве сервера).

12.1. Выбор уровня защиты от сетевых атак

Защита вашей работы в сети может осуществляться на одном из следующих уровней (см. рис. 42):

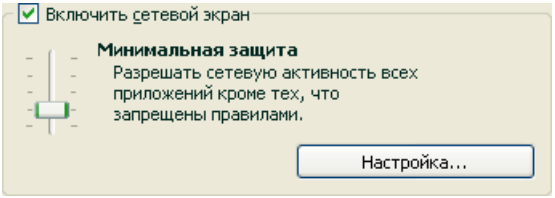


Рисунок 42. Выбор уровня сетевой защиты

Максимальная защита – уровень защиты, на котором разрешена сетевая активность, для которой предусмотрено разрешающее правило. Анти-Хакер использует правила, включенные в поставку или созданные вами. Набор правил, поставляемый вместе с Антивирусом Касперского, включает разрешающие правила для приложений, чья сетевая активность не вызывает подозрений, и пакетов данных, прием / передача которых абсолютно не опасны. Однако если в списке правил для приложения существует запрещающее правило более высокого приоритета, чем разрешающее, сетевая активность данного приложения будет запрещена.

> Внимание!
>
> На данном уровне защиты любое приложение, сетевая активность которого не зафиксирована в разрешающем правиле Анти-Хакера, будет блокироваться. Поэтому рекомендуется использовать этот уровень только в том случае, если вы уверены, что все необходимые для вашей работы программы разрешены соответствующими правилами и вы не планируете установку нового программного обеспечения.

Обучающий режим – уровень защиты, на котором происходит формирование правил Анти-Хакера. На данном уровне, каждый раз при попытке некоторой программы воспользоваться сетевым ресурсом, Анти-Хакер проверяет, есть ли для такого соединения правило. Если правило есть, Анти-Хакер действует в соответствии с его условиями. Если же правила нет, на экран выводится уведомление. Оно содержит описание сетевого соединения (какой программой инициируется, по какому порту и протоколу и т.д.). Вам необходимо принять решение, стоит ли разрешать такое соединение или нет. С помощью специальной кнопки в окне уведомления вы можете создать правило для такого соединения, чтобы впредь при аналогичном соединении Анти-Хакер использовал условия, заданные в нем, не выводя на экран уведомление.

Минимальная защита – уровень защиты, на котором блокируется только явным образом запрещенная сетевая активность. Анти-Хакер блокирует активность в соответствии с запрещающими правилами, включенными в поставку или созданными вами. Однако если в списке правил существует разрешающее правило для приложения более высокого приоритета, чем запрещающее, сетевая активность данного приложения будет разрешена.

Разрешить все – уровень защиты, разрешающий любую сетевую активность на вашем компьютере. Рекомендуется устанавливать такой уровень в крайне редких случаях, когда не наблюдается активных сетевых атак, и вы абсолютно доверяете любой сетевой активности.

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

Для того чтобы изменить уровень сетевой защиты,

1. Выберите компонент **Анти-Хакер** в окне настройки Антивируса Касперского.
2. В правой части окна переместите ползунок по шкале в разделе Сетевого экрана.

Для того чтобы настроить уровень сетевой защиты,

1. Выберите уровень защиты, наиболее близкий вашим предпочтениям.
2. Нажмите на кнопку **Настройка** и в открывшемся окне отредактируйте параметры сетевой защиты.

12.2. Правила для приложений

В поставку Антивируса Касперского включен набор правил для наиболее распространенных приложений под операционную систему Microsoft Windows. Для одной и той же программы может быть создано несколько правил как разрешающих, так и запрещающих. Как правило, это программы, сетевая активность которых детально проанализирована специалистами «Лаборатории Касперского» и строго определена как опасная или неопасная.

В зависимости от уровня защиты (см. п. 12.1 на стр. 155), выбранного для работы Сетевого экрана, и типа сети (см. п. 12.5 на стр. 166), в которой работает компьютер, список правил для программ используется по-разному. Так, например, на уровне **Максимальная защита** вся сетевая активность приложений, не подпадающая под разрешающие правила, блокируется.

Для работы со списком правил для приложений

1. Нажмите на кнопку **Настройка** в разделе Сетевого экрана окна настройки Анти-Хакера.
2. В открывшемся окне выберите закладку **Правила для приложений** (см. рис. 43).

Все правила на этой закладке могут быть сгруппированы одним из следующих способов:

- *Правила для приложений*. Установленный флажок ☑ **Группировать правила по приложениям** определяет такой способ представления списка правил. Закладка содержит список приложений, для которых сформированы правила. Для каждого приложения приводится следующая информация: имя и значок приложения, командная строка, корневой каталог, где расположен исполняемый файл приложения, и количество созданных для него правил

  По кнопке **Изменить** вы можете перейти к списку правил для выбранного в списке приложения и отредактировать его: добавить новое правило, изменить существующие и приоритет их выполнения.

  По кнопке **Добавить** вы можете добавить новое приложение в список и создать для него правила.

Кнопки **Экспорт** и **Импорт** предназначены для переноса сформированных правил на другие компьютеры. Это полезно для быстрой настройки Анти-Хакера.

- *Общий список правил* без группировки по имени приложения. Такой способ представления списка правил обуславливается снятым флажком **Группировать правила по приложениям**. Общий список правил отображает полную информацию правила: помимо имени приложения и командной строки его запуска будет указано действие правила (разрешать или запрещать сетевую активность), протокол передачи данных, направление потока данных (входящий или исходящий) и другая информация.

  По кнопке **Добавить** вы можете создать новое правило, по кнопке **Изменить –** перейти к редактированию выбранного в списке правила. Основные параметры правила вы также можете изменить в нижней части закладки.

  С помощью кнопок **Вверх** и **Вниз** вы можете изменить приоритет их выполнения.

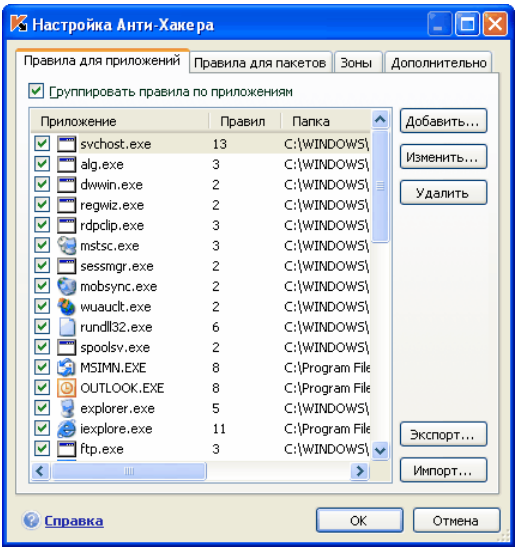


Рисунок 43. Список правил для установленных на компьютере приложений

12.2.1. Создание правила вручную

Чтобы создать правило для приложения вручную,

1. Выберите приложение. Для этого на закладке **Правила для приложений** (см. рис. 43) нажмите на кнопку **Добавить**. 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. В результате будет открыт список правил для выбранного приложения. Если для него уже существуют правила, все они будут приведены в верхней части окна. Если правил не существует, окно правил будет пустым.
2. В окне правил для выбранного приложения нажмите на кнопку **Добавить**.

Открывшееся окно **Новое правило** является формой для создания правила, где вы можете произвести тонкую настройку правила (см. п. 12.4 на стр. 162).

12.2.2. Создание правила на основе шаблона

В поставку приложения входят готовые шаблоны правил, которые вы можете использовать при создании собственных правил.

Все многообразие существующих сетевых приложений можно условно разделить на несколько типов: почтовые клиенты, веб-браузеры и т.п. Каждый тип характеризуется набором специфической активности, например, получение и отправка почты, получение и отображение HTML-страниц. Каждый тип использует определенный набор сетевых протоколов и портов. Таким образом, наличие шаблонов правил позволяет быстро и удобно производить начальную настройку правила исходя из типа приложения.

Чтобы создать правило для приложения, используя в качестве основы шаблон правил,

1. На закладке **Правила для приложений** установите флажок **Группировать правила по приложениям**, если он был снят, и нажмите на кнопку **Добавить**.
2. 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. В результате будет открыто окно правил для выбранного приложения. Если для него уже существуют

правила, все они будут приведены в верхней части окна. Если правил не существует, окно правил будет пустым.

3. В окне правил для приложения нажмите на кнопку **Шаблон** и из контекстного меню выберите один из шаблонов правила (см. рис. 44).

   Так, **Разрешить все** – правило, разрешающее любую сетевую активность приложения. **Запретить все** – правило, запрещающее любую сетевую активность приложения. Все попытки инициировать сетевое соединение приложением, для которой создано такое правило, будут блокироваться без предварительного уведомления пользователя.

   Остальные шаблоны, приведенные в контекстном меню, создают набор правил, характерных для соответствующих программ. Например, шаблон **Почтовый клиент** создает набор правил, разрешающих стандартную для почтового клиента сетевую активность, например, отправку почты.

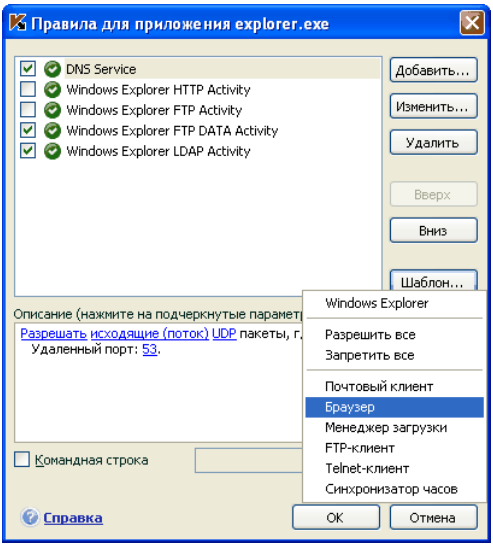


Рисунок 44. Выбор шаблона для создания нового правила

4. Откорректируйте созданные правила для приложения, если это необходимо. Вы можете изменить действие, направление сетевого соединения, удаленный адрес, порты (локальный и удаленный), а также время действия правила.

5. Если вы хотите, чтобы правило применялось к приложению, запущенному с определенными параметрами командной строки, уста-

новите флажок ☑ **Командная строка** и в поле справа введите строку.

Созданное правило (или набор правил) будет добавлено в конец списка с самым низким приоритетом. Вы можете повысить приоритет выполнения правила (см. п. 12.5 на стр. 166).

Создать правило можно также из окна уведомления об обнаружении сетевой активности (см. п. 12.10 на стр. 175).

12.3. Правила для пакетов

В поставку Антивируса Касперского включен набор правил, по которым осуществляется фильтрация передаваемых и принимаемых вашим компьютером пакетов данных. Передача пакетов может быть инициирована вами или каким-либо приложением, установленным на вашем компьютере. В поставку приложения входят правила фильтрации для пакетов, передача которых детально проанализирована специалистами «Лаборатории Касперского» и строго определена как опасная или неопасная.

В зависимости от уровня защиты, выбранного для работы Сетевого экрана, и типа сети, в которой работает компьютер, список правил используется по-разному. Так, например, на уровне **Максимальная защита** вся сетевая активность, не попадающая под разрешающие правила, блокируется.

Важно!

Обратите внимание, что правила для зон безопасности (см. п. 12.6 на стр. 167) имеют более высокий приоритет, чем запрещающие пакетные правила. Так, например, при выборе статуса **Локальная сеть** будет разрешен обмен пакетами, а также доступ к папкам общего доступа, независимо от наличия запрещающих пакетных правил.

Для работы со списком правил для пакетов:

1. Нажмите на кнопку **Настройка** в разделе Сетевого экрана окна настройки Анти-Хакера.
2. В открывшемся окне выберите закладку **Правила для пакетов** (см. рис. 45).

Для каждого правила фильтрации приводится следующая информация: имя правила, действие (разрешающее или запрещающее передачу пакета), протокол передачи данных, направление пакета, а также параметры сетевого соединения, по которому выполняется передача пакета.

Использование правила фильтрации в настоящий момент регулируется флажком рядом с его именем.

Работа со списком правил ведется посредством кнопок, расположенных справа от списка.

Чтобы создать новое пакетное правило,

на закладке **Правила для пакетов** нажмите на кнопку **Добавить**.

Открывшееся окно **Новое правило** является формой для создания правила, где вы можете произвести тонкую настройку правила (см. п. 12.4 на стр. 162).

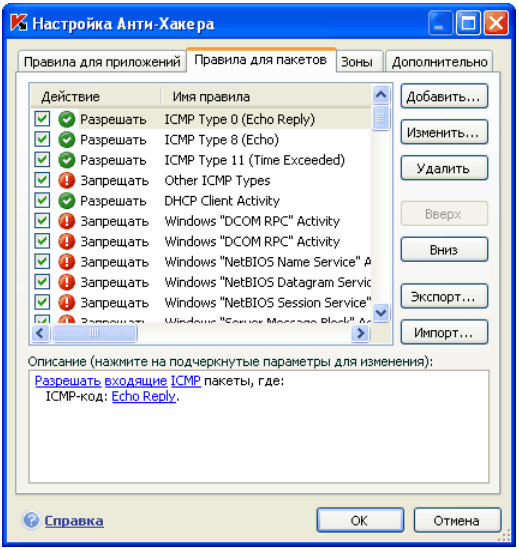


Рисунок 45. Список правил для пакетной фильтрации

12.4. Тонкая настройка правил для приложений и пакетов

Окно подробной настройки правил **Новое правило** (см. рис. 46) практически одинаково для приложений и пакетов.

Первым шагом является:

- Определение имени правила. По умолчанию приложение использует стандартное имя, которое вы можете изменить.

- Выбор параметров сетевого соединения, в соответствии с которыми будет действовать правило: удаленный IP-адрес, удаленный порт, локальный IP-адрес и время действия правила. Установите флажки для тех из них, которые вы хотите использовать в правиле.

- Задание дополнительных параметров, отвечающих за информирование пользователя о применении правила. Если вы хотите, чтобы при выполнении правила на экране открывалось всплывающее сообщение, кратко комментирующее его, установите флажок **Показывать предупреждение**. Для того чтобы информация о выполнении правила фиксировалась в отчете Анти-Хакера, установите флажок **Записывать в отчет**. По умолчанию при создании правила флажок не установлен. Рекомендуем вам использовать дополнительные параметры при создании запрещающих правил.

Обратите внимание, что при создании запрещающего правила в режиме обучения Анти-Хакера информация о применении правила автоматически заносится в отчет. Если фиксировать данную информацию не требуется, снимите флажок **Записывать в отчет** в параметрах данного правила.

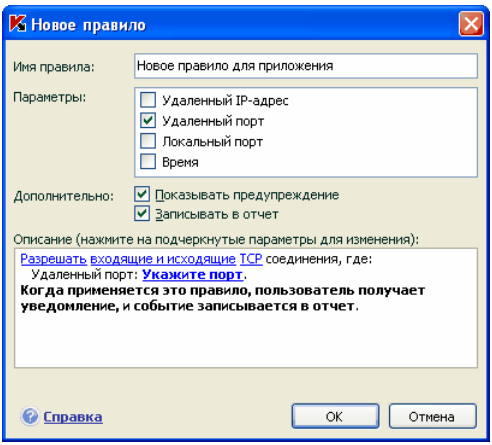


Рисунок 46. Создание нового правила для приложения

Вторым шагом в создании правила является задание значений для параметров правила и выбор действия. Эти операции выполняются в разделе **Описание**.

1. Действие каждого создаваемого правила – *разрешающее*. Чтобы заменить его на запрещающее правило, в разделе описания правила щелкните левой клавишей мыши по ссылке Разрешать. Она примет значение Запрещать.

Сетевой трафик для приложений и пакетов, для которых было создано разрешающее правило, все равно будет проверяться Антивирусом Касперского. Вследствие этого возможно снижение скорости передачи данных.

2. Если вы создаете правило для приложения и перед началом его создания вы не указали приложение, вам нужно будет сделать это посредством ссылки укажите приложение. Щелкните левой клавишей мыши по ссылке и в открывшемся стандартном окне выбора файлов выберите исполняемый файл приложения, для которого создается правило.

3. Затем вам нужно определить направление сетевого соединения для правила. По умолчанию предлагается создать правило как для входящего, так и для исходящего сетевого соединения. Чтобы изменить направление, щелкните левой клавишей мыши по ссылке входящие и исходящие и в открывшемся окне выберите направление сетевого соединения:

   - **Входящий поток**. Правило применяется для сетевого соединения, открытого удаленным компьютером.
   - **Входящий пакет**. Правило применяется для пакетов данных, принимаемым вашим компьютером, за исключением TCP-пакетов.
   - **Входящий и исходящий потоки**. Правило применяется как ко входящему, так и к исходящему потоку информации, независимо от того, каким компьютером (вашим или удаленным) было инициировано сетевое соединение.
   - **Исходящий поток**. Правило применяется только для сетевого соединения, открытого вашим компьютером.
   - **Исходящий пакет**. Правило применяется для входящих пакетов данных, передаваемых с вашего компьютера, за исключением TCP-пакетов.

   Если в правиле вам важно зафиксировать направление именно пакета, определите, исходящий это пакет или входящий. Если же вы хотите создать правило для потока данных, выберите тип потока: входящий, исходящий или и тот и другой.

   Отличие *направления потока* от *направления пакета* состоит в том, что при создании правила для потока определяется, в каком направлении будет открыто соединение. Направление пакетов при передаче данных по этому соединению не учитывается.

   Например, если вы настраиваете правило для обмена данными с FTP-сервером, работающим в пассивном режиме, вам нужно разрешить исходящий поток. Для обмена данными с FTP-сервером в

активном режиме необходимо разрешить как исходящий, так и входящий поток.

4. Если в качестве параметра сетевого соединения вы выбрали удаленный адрес, щелкните левой клавишей мыши по ссылке укажите адрес и в открывшемся окне задайте IP-адрес, диапазон адресов или адрес подсети. Для одного правила вы можете использовать как один тип IP-адреса, так и несколько типов. Можно задавать несколько адресов каждого типа.

5. Далее вам нужно определить протокол, по которому выполняется сетевое соединение. По умолчанию предлагается использовать соединение по TCP-протоколу. При создании правила для приложения вы можете выбирать один из двух типов протоколов – TCP или UDP. Для этого щелкните левой клавишей мыши по ссылке с названием протокола пока она не примет нужное вам значение. Если вы создаете правило для пакета и хотите изменить тип протокола по умолчанию, щелкните по ссылке с его именем и в открывшемся окне укажите требующийся тип протокола. При выборе ICMP-протокола вам может понадобиться дополнительно указать его тип.

6. Если вы выбрали параметры сетевого соединения (адрес, порт, время правила), вам также необходимо задать для них точные значения.

После того как правило добавлено в список правил для приложения, вы можете провести дополнительную настройку правила (см. рис. 47). Если вы хотите, чтобы оно применялось к приложению, запущенному с определенными параметрами командной строки, установите флажок ☑ **Командная строка** и в поле справа введите строку. Для приложения, запущенного с другим ключом командной строки, данное правило выполняться не будет.

Возможность запуска приложения с определенными параметрами командной строки недоступна для операционной системы Microsoft Windows 98.

Создать правило можно также из окна уведомления об обнаружении сетевой активности (см. п. 12.10 на стр. 175).

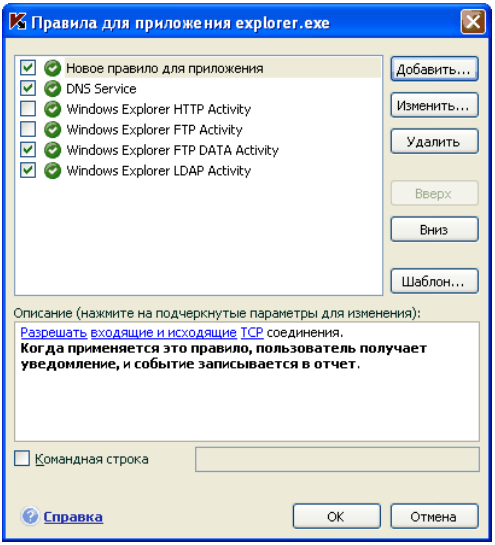


Рисунок 47. Дополнительная настройка нового правила

12.5. Изменение приоритета правила

Для каждого правила, созданного для приложения или пакета, установлен приоритет выполнения. При прочих равных условиях (например, параметрах сетевого соединения) к сетевой активности приложения будет применено то действие, которое определено правилом с наибольшим приоритетом.

Приоритет правила определяется его положением в списке правил. Самое первое правило в списке обладает самым высоким приоритетом выполнения. Каждое создаваемое вручную правило добавляется в начало списка. Правила, формируемые на основе шаблона или из специального уведомления, добавляются в конец списка правил.

Чтобы изменить приоритет правила для приложения, выполните следующие действия:

1. Выберите имя приложения на закладке **Правила для приложений** и нажмите на кнопку **Изменить**.
2. Используйте кнопки **Вверх** и **Вниз** в открывшемся окне созданных для приложения правил, чтобы переместить их по списку, меняя таким образом их приоритет.

Чтобы изменить приоритет правила для пакета, выполните следующие действия:

1. Выберите правило на закладке **Правила для пакетов**.
2. Используйте кнопки **Вверх** и **Вниз**, чтобы перемещать правила в списке, изменяя таким образом их приоритет.

12.6. Правила для зон безопасности

После установки приложения компонент Анти-Хакер проводит анализ сетевого окружения вашего компьютера. По результатам анализа все сетевое пространство делится на условные зоны:

Интернет – глобальная сеть Интернет. В данной зоне Антивирус Касперского работает как персональный сетевой экран. При этом вся сетевая активность регламентируется правилами для пакетов и приложений, созданными по умолчанию для обеспечения максимальной безопасности. Вы не можете изменять условия защиты при работе в данной зоне, кроме как включить режим невидимости компьютера для дополнительной безопасности.

Зоны безопасности – некоторые условные зоны, зачастую совпадающие с подсетями, в которые включен ваш компьютер (это могут быть локальные подсети дома или на работе). По умолчанию данные зоны считаются зонами средней степени риска при работе в них. Вы можете изменять статус данных зон исходя из степени доверия той или иной подсети, а также настраивать правила для пакетов и приложений.

Если включен режим обучения Анти-Хакера, при каждом подключении компьютера к некоторой новой зоне будет выводиться окно, содержащее ее краткое описание. Вам нужно присвоить статус данной зоне, на основании которого будет разрешена та или иная сетевая активность:

- **Интернет**. Этот статус по умолчанию присваивается сети Интернет, поскольку при работе в ней компьютер подвержен любым возможным типам угроз. Также данный статус рекомендуется выбирать для сетей, не защищенных какими-либо антивирусными приложениями, сетевыми экранами, фильтрами и т.д. При выборе этого статуса обеспечивается максимальная безопасность работы компьютера в данной зоне, а именно:
    - блокируется любая сетевая NetBios-активность в рамках подсети;

- запрещается выполнение правил для приложений и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

Даже если вы создали папку общего доступа, информация, содержащаяся в ней, не будет доступна пользователям подсети с таким статусом. Кроме того, при выборе данного статуса вы не сможете получить доступ к файлам и принтерам на других компьютерах сети.

- **Локальная сеть**. Этот статус присваивается по умолчанию всем зонам, обнаруженным при анализе сетевого окружения компьютера, за исключением сети Интернет. Рекомендуется применять этот статус для зон со средней степенью риска работы в них (например, для внутренней корпоративной сети). При выборе данного статуса разрешается:

  - любая сетевая NetBios-активность в рамках подсети;
  - выполнение правил для приложений и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

  Выбирайте этот статус, если вы хотите предоставить доступ к некоторым каталогам или принтерам на вашем компьютере, но запретить любую другую внешнюю активность.

- **Доверенная**. Этот статус рекомендуется применять только для абсолютно безопасной, по вашему мнению, зоны, при работе в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. При выборе такого статуса будет разрешена любая сетевая активность. Даже если установлен уровень Максимальной защиты и созданы запрещающие правила, они не будут действовать для удаленных компьютеров доверенной зоны.

Обратите внимание на то, что любые ограничения доступа на работу к файлам действуют только в рамках указанной подсети.

Для сети со статусом **Интернет** вы можете для дополнительной безопасности использовать режим невидимости. В этом режиме разрешена только сетевая активность, инициированная с вашего компьютера. Фактически это означает, что ваш компьютер становится «невидимым» для внешнего окружения. В то же время на вашу работу в интернете режим не оказывает никакого влияния.

Внимание!

Не рекомендуется использовать режим невидимости, если компьютер используется в качестве сервера (например, почтового, http-сервера). Иначе, компьютеры, обращающиеся к данному серверу, не будут видеть его в сети.

Список зон, в которых был зарегистрирован ваш компьютер, отображается на закладке **Зоны** (см. рис. 48). Для каждой из них приведен статус, дано краткое описание сети и указано, используется или нет режим невидимости.

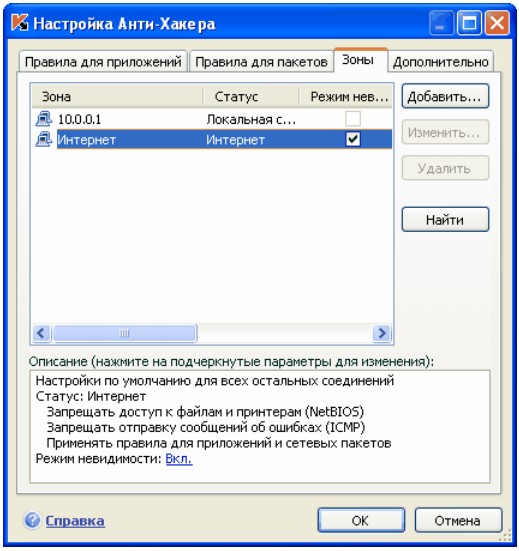


Рисунок 48. Список правил для зон

Чтобы изменить статус зоны либо включить / отключить режим невидимости, выберите ее в списке и в блоке **Описание**, расположенном под списком, воспользуйтесь соответствующими ссылками. Аналогичные действия, а также редактирование адреса и маски подсети можно выполнить в окне **Параметры зоны**, открывающемся по кнопке **Изменить**.

При просмотре списка зон вы можете добавить в него новую, для этого воспользуйтесь кнопкой **Найти**. Анти-Хакер произведет поиск возможных для регистрации зон и, если таковые будут обнаружены, предложит вам определить их статус. Кроме того, вы можете добавить новую зону в список вручную (например, в случае, когда вы включаете мобильный компьютер в новую сеть). Для этого воспользуйтесь кнопкой **Добавить** и укажите требующуюся информацию в окне **Параметры зоны**.

Чтобы удалить сеть из списка, воспользуйтесь кнопкой **Удалить**.

12.7. Режим работы сетевого экрана

Режим работы сетевого экрана (см. рис. 49) регламентирует совместимость Анти-Хакера с программами, устанавливающими множественные сетевые соединения, а также с сетевыми играми.

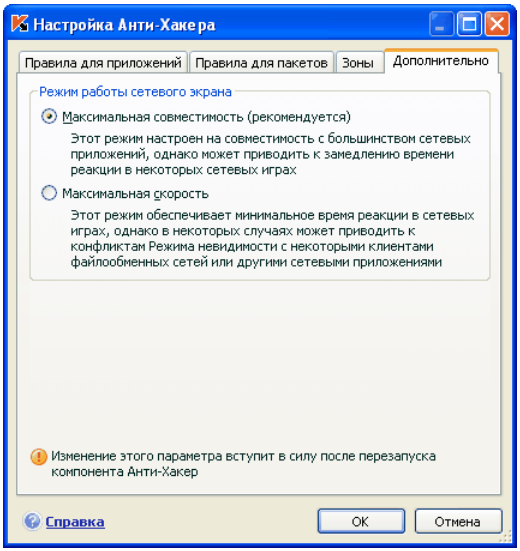


Рисунок 49. Выбор режима работы Анти-Хакера

Максимальная совместимость – режим работы сетевого экрана, обеспечивающий оптимальную работу компонента Анти-Хакер и программ, устанавливающих множественные сетевые соединения (клиенты файлообменных сетей). Однако использование данного режима в некоторых случаях может приводить к замедлению времени реакции в сетевых играх. При возникновении подобной ситуации рекомендуется использовать режим Максимальная скорость.

Максимальная скорость – режим работы сетевого экрана, обеспечивающий максимальную скорость реакции во время сетевых игр. Однако в данном режиме возможны конфликты в работе клиентов файлообменных сетей или других сетевых приложений. Для решения проблемы рекомендуется отключить режим невидимости.

Чтобы настроить режим работы сетевого экрана,

1. Откройте окно настройки приложения и выберите компонент **Анти-Хакер** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в разделе Сетевого экрана окна настройки Анти-Хакера.
3. В открывшемся окне выберите закладку **Дополнительно** и установите нужный режим работы – Максимальная совместимость или Максимальная скорость.

Изменение режима работы сетевого экрана вступит в силу только после перезапуска компонента Анти-Хакер.

12.8. Настройка системы обнаружения вторжений

Все известные на настоящее время сетевые атаки, которым подвержен компьютер, приведены в сигнатурах угроз. На основе списка этих атак работает **модуль обнаружения вторжений** компонента Анти-Хакер. Пополнение списка атак, обнаруживаемых этим модулем, выполняется в процессе обновления сигнатур. По умолчанию Антивирус Касперского не обновляет сигнатуры атак (см. 16.4.2 на стр. 232).

Система обнаружения вторжений отслеживает сетевую активность, характерную для сетевых атак, и при обнаружении попытки атаковать ваш компьютер блокирует любого рода сетевую активность атакующего компьютера в отношении вашего компьютера на один час. На экран выводится уведомление о том, что была произведена попытка сетевой атаки с указанием информации об атакующем компьютере.

Вы можете настроить работу Системы обнаружения атак. Для этого:

1. Откройте окно настройки приложения и выберите компонент **Анти-Хакер** в разделе **Защита**.
2. В разделе **Система обнаружения вторжений** нажмите на кнопку **Настройка**.
3. В открывшемся окне (см. рис. 50) определите, нужно ли блокировать атакующий компьютер и если да, то на какое время. По умолчанию атакующий компьютер блокируется на 60 минут. Вы можете сократить или увеличить время блокировки, изменив значение поля рядом с флажком **Блокировать атакующий компьютер на ... мин.** Если вы хотите отказаться от блокировки сетевой актив-

ности атакующего компьютера в отношении вашего компьютера, снимите этот флажок.

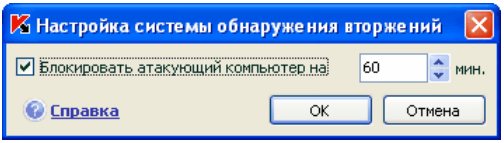


Рисунок 50. Настройка времени блокирования атакующего компьютера

12.9. Список обнаруживаемых сетевых атак

В настоящее время существует множество различных видов сетевых атак, которые используют как уязвимости операционной системы, так и иного установленного программного обеспечения системного и прикладного характера. Злоумышленники постоянно совершенствуют методы нападения, результатом которых могут являться кража конфиденциальной информации, выведение системы из строя либо ее полный «захват» с последующим использованием как части зомби-сети для совершения новых атак.

Для того чтобы своевременно обеспечить безопасность компьютера, важно знать, какого рода сетевые атаки могут угрожать ему. Известные сетевые угрозы можно условно разделить на три большие группы:

- **Сканирование портов** – этот вид угроз сам по себе не является атакой, а обычно предшествует ей, поскольку является одним из основных способов получить сведения об удаленном компьютере. Этот способ заключается в сканировании UDP / TCP-портов, используемых сетевыми сервисами на интересующем компьютере, для выяснения их состояния (закрытые или открытые порты).

  Сканирование портов позволяет понять, какие типы атак на данную систему могут оказаться удачными, а какие нет. Кроме того, полученная в результате сканирования информация («слепок» системы) даст представление злоумышленнику о типе операционной системы на удаленном компьютере. А это, в свою очередь, еще сильнее ограничивает круг потенциальных атак и, соответственно, время, затрачиваемое на их проведение, а также позволяет попытаться использовать специфические для данной операционной системы уязвимости.

- **DoS-атаки или атаки, вызывающие отказ в обслуживании** – это атаки, результатом которых является приведение атакуемой системы в нестабильное, либо полностью нерабочее состояние. Последствиями такого типа атак могут стать повреждение или разрушение

информационных ресурсов, на которые они направлены, и, следовательно, невозможность их использования.

Существует два основных типа DoS атак:

- отправка компьютеру-жертве специально сформированных пакетов, не ожидаемых этим компьютером, что приводит к перезагрузке или остановке системы;
- отправка компьютеру-жертве большого количества пакетов в единицу времени, которые этот компьютер не в состоянии обработать, что приводит к исчерпанию ресурсов системы.

Яркими примерами данной группы атак являются следующие атаки:

- *Атака Ping of death* состоит в посылке ICMP-пакета, размер которого превышает допустимое значение в 64 КБ. Эта атака может привести к аварийному завершению работы некоторых операционных систем.
- *Атака Land* заключается в передаче на открытый порт вашего компьютера запроса на установление соединения с самим собой. Атака приводит к зацикливанию компьютера, в результате чего сильно возрастает загрузка процессора и возможно аварийное завершение работы некоторых операционных систем.
- *Атака ICMP Flood* заключается в отправке на ваш компьютер большого количества ICMP-пакетов. Атака приводит к тому, что компьютер вынужден отвечать на каждый поступивший пакет, в результате чего сильно возрастает загрузка процессора.
- *Атака SYN Flood* заключается в отправке на ваш компьютер большого количества запросов на установку соединения. Система резервирует определенные ресурсы для каждого из таких соединений, в результате чего тратит свои ресурсы полностью и перестает реагировать на другие попытки соединения.

- **Атаки-вторжения**, целью которых является «захват» системы. Это самый опасный тип атак, поскольку в случае успешного выполнения система оказывается полностью скомпрометированной перед злоумышленником.

  Данный тип атак применяется, когда необходимо получить конфиденциальную информацию с удаленного компьютера (например, номера кредитных карт, пароли) либо просто закрепиться в системе для последующего использования ее вычислительных ресурсов в целях злоумышленника (использование захваченной системы в зомби-сетях либо как плацдарма для новых атак).

Данная группа является также самой большой по количеству включенных в нее атак. Их можно разделить на три подгруппы в зависимости от операционной системы: атаки под Microsoft Windows, атаки под Unix, а также общая группа для сетевых сервисов, использующихся в обеих операционных системах.

Наиболее распространенными видами атак, использующих сетевые сервисы операционной системы, являются:

- *атаки на переполнение буфера* – тип уязвимостей в программном обеспечении, возникающий из-за отсутствия контроля (либо недостаточном контроле) при работе с массивами данных. Это один из самых старых типов уязвимостей и наиболее простой для эксплуатации злоумышленником.

- *атаки, основанные на ошибках форматных строк* – тип уязвимостей в программном обеспечении, возникающий из-за недостаточного контроля значений входных параметров функций форматного ввода-вывода типа *printf()*, *fprintf()*, *scanf()* и прочих из стандартной библиотеки языка Си. Если подобная уязвимость присутствует в программном обеспечении, то злоумышленник, имея возможность посылать специальным образом сформированные запросы, может получить полный контроль над системой.

Система обнаружения вторжений автоматически анализирует и предотвращает использование подобных уязвимостей в наиболее распространенных сетевых сервисах (FTP, POP3, IMAP), в случае если они функционируют на компьютере пользователя.

Атаки под операционную систему Microsoft Windows основаны на использовании уязвимостей установленного на компьютере программного обеспечения (например, таких программ как Microsoft SQL Server, Microsoft Internet Explorer, Messenger, а также системных компонентов, доступных по сети, – DCom, SMB, Wins, LSASS, IIS5).

Например, компонент Анти-Хакер защищает компьютер от атак, использующих следующие известные уязвимости программного обеспечения (список уязвимостей приведен в соответствии с нумерацией Microsoft Knowledge Base):

(**MS03-026**) DCOM RPC Vulnerability (Lovesan worm)

(**MS03-043**) Microsoft Messenger Service Buffer Overrun

(**MS03-051**) Microsoft Office Frontpage 2000 Server Extensions Buffer Overflow

(**MS04-007**) Microsoft Windows ASN.1 Vulnerability

(**MS04-031**) Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow

(**MS04-032**) Microsoft Windows XP Metafile (.emf) Heap Overflow

(**MS05-011**) Microsoft Windows SMB Client Transaction Response Handling

(**MS05-017**) Microsoft Windows Message Queuing Buffer Overflow Vulnerability

(**MS05-039**) Microsoft Windows Plug-and-Play Service Remote Overflow

(**MS04-045**) Microsoft Windows Internet Naming Service (WINS) Remote Heap Overflow

(**MS05-051**) Microsoft Windows Distributed Transaction Coordinator Memory Modification

Кроме того, частными случаями атак-вторжений являются использование различного вида вредоносных скриптов, в том числе скриптов, обрабатываемых Microsoft Internet Explorer, а также разновидности червя Helkern. Суть последнего типа атаки заключается в отправке на удаленный компьютер UDP-пакета специального вида, способного выполнить вредоносный код.

Помните, что при работе в сети ваш компьютер ежедневно подвергается риску быть атакованным со стороны злоумышленников. Чтобы обеспечить безопасную работу компьютера обязательно включайте компонент Анти-Хакер при работе в интернете и регулярно обновляйте сигнатуры хакерских атак (см. п. 16.4.2 на стр. 232).

12.10. Разрешение / запрещение сетевой активности

Если в качестве уровня защиты для сетевого экрана выбран **Обучающий режим**, каждый раз при попытке выполнить сетевое соединение, для которого не сформировано правило, на экран выводится специальное уведомление.

Например, если для работы с электронной почтой вы используете Microsoft Office Outlook, после открытия данный почтовый клиент подгружает вашу почту с удаленного Exchange-сервера. Для того чтобы отобразить ваш почтовый ящик, приложение выполняет сетевое соединение с почтовым сервером. Такая сетевая активность обязательно будет отслежена Анти-Хакером. В этом случае на экран будет выведено сообщение (см. рис. 51), содержащее:

- *Описание активности* – название приложения и краткая характеристика соединения, которое оно инициирует. Как правило, указывается тип соединения, локальный порт, с которого оно инициируется, удаленный порт и адрес, с которым выполняется соединение. Для получения подробной информации о соединении, о процессе, кото-

рый его инициирует, и о компании-производителе приложения щелкните левой клавишей мыши в любом месте блока.

- *Действие* – последовательность операций, которую следует выполнить Анти-Хакеру в отношении обнаруженной сетевой активности.

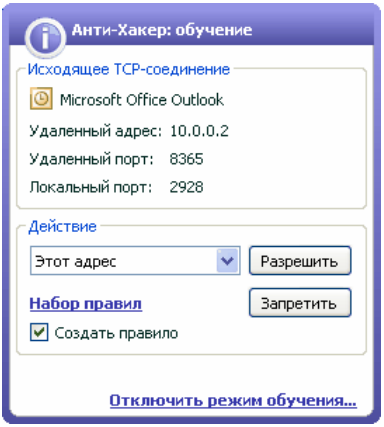


Рисунок 51. Уведомление о сетевой активности

Внимательно изучите информацию о сетевой активности и только после этого выберите действие Анти-Хакера. Рекомендуем вам воспользоваться следующими советами при принятии решения:

1. Прежде всего определите, разрешить или запретить сетевую активность. Возможно, в данном случае вам поможет набор правил, уже сформированных для данного приложения или пакета (при условии, что они созданы). Для этого воспользуйтесь ссылкой **Набор правил**. В результате будет открыто окно с полным списком правил, сформированных для приложения или пакета данных.
2. Затем определите, разово выполнить действие или автоматически выполнять его каждый раз при обнаружении такой активности.

Для разового выполнения действия

снимите флажок **Создать правило** и нажмите на кнопку с именем действия, например, на кнопку **Разрешить**.

Чтобы выбранное вами действие выполнялось автоматически каждый раз, когда такая активность будет инициироваться на вашем компьютере,

1. Убедитесь, что флажок **Создать правило** установлен.
2. Выберите тип активности, к которой вы хотите применить действие, из раскрывающегося списка блока **Действие**:

- **Любая активность** – сетевая активность любого характера, инициируемая данным приложением.
- **Выборочно** – отдельная активность, которую вам нужно определить в окне создания правила (см. п. 12.2.1 на стр. 159).
- **<Шаблон>** – имя шаблона, включающего набор правил, характерных для сетевой активности приложения. Такой тип активности появляется в списке в том случае, если для приложения, инициировавшего сетевую активность, существует подходящий шаблон, включенный в поставку Антивируса Касперского (см. п. 12.2.2 на стр. 159). В этом случае вам не нужно выборочно определять, какую же активность разрешить или запретить в данный момент. Воспользуйтесь шаблоном, и набор правил для приложения будет создан автоматически.

3. Нажмите на кнопку с именем действия (**Разрешить** или **Запретить**).

Помните, что созданное правило будет использоваться только в случае, когда все параметры соединения ему удовлетворяют. Для соединения, выполняемого, например, с другого локального порта, такое правило будет недействительно.

Чтобы отключить получение уведомлений от Анти-Хакера при попытках любого приложения установить сетевое соединение, воспользуйтесь ссылкой Отключить режим обучения. После этого Анти-Хакер будет переведен в режим Минимальной защиты, в рамках которого разрешены любые сетевые соединения за исключением тех, которые явно запрещены правилами.

ГЛАВА 13. ЗАЩИТА ОТ НЕЖЕЛАТЕЛЬНОЙ ПОЧТЫ

В состав Антивируса Касперского 6.0 включен специальный компонент, позволяющий обнаруживать нежелательную корреспонденцию (спам) и обрабатывать ее в соответствии с правилами вашего почтового клиента, экономя ваше время при работе с электронной почтой.

Проверка почтового сообщения на спам производится по следующему алгоритму:

1. Адрес отправителя почтового сообщения проверяется на присутствие в «черном» или «белом» списке адресов.
    - Если адрес отправителя находится в «белом» списке, письму присваивается статус *не спам*.
    - Если адрес отправителя находится в «черном» списке, почтовому сообщению присваивается статус *спам*. Дальнейшая обработка письма зависит от выбранного вами действия (см. п. 13.3.7 на стр. 197).
2. Если адрес отправителя не обнаружен в «черном» или «белом» списке, производится анализ почтового сообщения с помощью технологии PDB (см. п. 13.3.2 на стр. 188).
3. Анти-Спам подробно изучает текст почтового сообщения и проверяет его на наличие строк из «черного» и «белого» списков.
    - Если текст письма содержит строки из «белого» списка строк, письму присваивается статус *не спам*.
    - Если в тексте встречаются строки из «черного» списка строк, почтовому сообщению присваивается статус *спам*. Дальнейшая обработка письма зависит от выбранного вами действия.
4. Если почтовое сообщение не содержит строк, приведенных в «черном» и «белом» списках, выполняется его анализ на фишинг. Если текст письма содержит адрес, входящий в базу антифишинга, письму присваивается статус *спам*. Дальнейшая обработка письма зависит от выбранного вами действия.
5. Если почтовое сообщение не содержит фишинг-строк, выполняется его анализ на спам с помощью специальных технологий:
    - анализ изображений по технологии GSG;

- анализ текста сообщения с применением алгоритма распознавания спама – алгоритма iBayes.

6. После этого выполняется проверка дополнительных признаков фильтрации спама (см. п. 13.3.5 на стр. 195), установленных пользователем при настройке Анти-Спама. В их число, например, может входить: проверка корректности HTML-тегов, размера текста, невидимых символов.

Каждый из приведенных выше этапов, которые проходит письмо при анализе на спам, вы можете отключить.

Анти-Спам встраивается в виде модуля расширения в следующие почтовые клиенты:

- Microsoft Office Outlook (см. п. 13.3.8 на стр. 198).
- Microsoft Outlook Express (Windows Mail) (см. п. 13.3.9 на стр. 201).
- The Bat! (см. п. 13.3.10 на стр. 203).

В данной версии Антивируса Касперского не предусмотрен модуль расширения Анти-Спама для Microsoft Office Outlook, установленного под Microsoft Windows 98.

В панели задач почтовых клиентов Microsoft Office Outlook и Microsoft Outlook Express (Windows Mail) вы найдете две кнопки **Спам** и **Не Спам**, которые позволяют настраивать Анти-Спам на распознавание нежелательной почты в контексте именно вашей корреспонденции. В The Bat! такие кнопки отсутствуют, однако обучение можно проводить с помощью специальных пунктов **Пометить как спам** и **Пометить как НЕ спам** в меню **Специальное**. Также ко всем параметрам почтового клиента добавляются специальные параметры обработки нежелательной почтовой корреспонденции (см. п. 13.3.1 на стр. 187).

Анти-Спам использует модифицированный самообучающийся алгоритм iBayes, что позволяет компоненту с течением времени более точно различать *спам* и *полезную почту*. Источником данных для алгоритма является содержимое письма.

Возникают ситуации, когда модифицированный самообучающийся алгоритм iBayes не способен с большой долей вероятности отнести некоторое электронное сообщение ни к спаму, ни к полезной почте. Такое электронное письмо получает статус *потенциального спама*.

Чтобы снизить объем почтовых сообщений, являющихся потенциальным спамом, рекомендуется провести дополнительное обучение Анти-Спама на таких письмах (см. п. 13.2 на стр. 182). Для этого необходимо указать, какие из этих писем стоит относить к *спаму*, а какие – к *не спаму*.

Электронные сообщения, являющиеся *спамом* или *потенциальным спамом*, модифицируются: в поле **Тема** письма добавляется метка **[!! SPAM]** или **[?? Probable Spam]**, соответственно.

Правила обработки почтовых сообщений, отмеченных как спам или потенциальный спам, для почтовых клиентов Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail) и The Bat! задаются в специальных модулях расширения, созданных для этих клиентов. Для других почтовых клиентов вы можете настроить правила фильтрации, чтобы они учитывали поле **Тема** письма и, например, в зависимости от наличия в нем метки **[!! SPAM]** или **[?? Probable Spam]**, перемещали электронное письмо в соответствующую папку. Для более подробного ознакомления с механизмами фильтрации обратитесь к документации по вашему почтовому клиенту.

13.1. Выбор уровня агрессивности Анти-Спама

Антивирус Касперского обеспечивает защиту от спама на одном из следующих уровней (см. рис. 52):

Блокировать все – самый строгий уровень агрессивности, на котором спамом признается любая почта, кроме сообщений, содержащих строки из «белого» списка фраз и отправители которых перечислены в «белом» списке адресов (см. п. 13.3.4.1 на стр. 191). На данном уровне анализ письма выполняется только по «белому» списку, использование остальных технологий отключено.

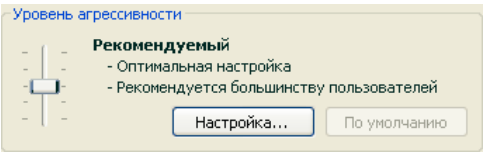


Рисунок 52. Выбор уровня защиты от спама

Высокий – строгий уровень, при активации которого возникает вероятность того, что некоторые электронные письма, не являющиеся на самом деле спамом, будут помечены как *спам*. На данном уровне анализ письма выполняется по «белому» и «черному» спискам, а также с использованием технологий PDB и GSG, а также алгоритма iBayes (см. п. 13.3.2 на стр. 188).

Данный режим имеет смысл применять в тех случаях, когда высока вероятность того, что адрес получателя корреспонденции неизвестен спамерам. Например, когда получатель не зарегистрирован в почтовых

рассылках и не имеет почтовый ящик на бесплатных / не корпоративных почтовых серверах.

Рекомендуемый – наиболее универсальный уровень настройки с точки зрения классификации электронных сообщений.

При таком уровне возможно возникновение ситуаций, когда нежелательные письма не будут распознаны. Это указывает на то, что Анти-Спам недостаточно хорошо обучен. Рекомендуется провести дополнительное обучение модуля с помощью Мастера обучения (см. п. 13.2.1 на стр. 182) или кнопок **Спам** \ **Не спам** (для программы The Bat! – пункты меню) на тех письмах, которые были распознаны неверно.

Низкий – более лояльный уровень настройки. Он может быть рекомендован тем пользователям, чья входящая корреспонденция по каким-либо причинам содержит значительное количество слов, распознаваемых Анти-Спамом как спам, но таковым не являющаяся. Причиной такой ситуации может служить профессиональная деятельность получателя, в силу которой он вынужден использовать в своей переписке с коллегами профессиональные термины, широко встречающиеся в спаме. Для анализа сообщений на данном уровне используются все технологии обнаружения спама.

Пропускать все – самый низкий уровень агрессивности, на котором спамом признается только та почта, которая содержит строки из «черного» списка фраз и отправители которой перечислены в «черном» списке адресов. На данном уровне анализ письма выполняется только по «черному» списку, использование остальных технологий отключено.

По умолчанию защита от спама осуществляется на **Рекомендуемом** уровне агрессивности.

Вы можете повысить или понизить уровень, или изменить параметры текущего уровня.

Для того чтобы изменить уровень,

переместите ползунок по шкале уровней агрессивности. Регулируя уровень агрессивности, вы определяете соотношение факторов спама, потенциального спама и полезной почтой (см. п. 13.3.3 на стр. 189).

Чтобы изменить параметры текущего уровня,

нажмите на кнопку **Настройка** в окне настройки Анти-Спама, в открывшемся окне откорректируйте фактор спама и нажмите на кнопку **ОК**.

В результате уровень защиты изменится на **Пользовательский**, содержащий параметры защиты, заданные вами.

13.2. Обучение Анти-Спама

Анти-Спам поставляется с предустановленной базой писем, состоящей из пятидесяти спам-писем. Рекомендуется провести дополнительное обучение модуля Анти-Спам на ваших почтовых сообщениях.

Существует несколько подходов к обучению Анти-Спама:

- Использование Мастера обучения (пакетное обучение) (см. п. 13.2.1 на стр. 182).
- Обучение Анти-Спама на исходящих сообщениях (см. п. 13.2.2 на стр. 183).
- Обучение непосредственно во время работы с электронной корреспонденцией, используя специальные кнопки в панели инструментов почтового клиента или пункты меню (см. п. 13.2.3 на стр. 184).
- Обучение при работе с отчетами Анти-Спама (см. п. 13.2.4 на стр. 185).

Обучение с помощью Мастера обучения предпочтительно в самом начале работы с Анти-Спамом. Мастер позволяет обучить Анти-Спам на большом количестве электронных писем.

Обратите внимание, что количество писем для обучения из одной папки не может превышать 50. Если в папке писем больше, обучение будет выполнено только на пятидесяти.

Дополнительное обучение с помощью специальных кнопок в интерфейсе почтового клиента предпочтительно использовать во время непосредственной работы с электронной корреспонденцией.

13.2.1. Мастер обучения

Мастер обучения позволяет провести обучение Анти-Спама в пакетном режиме, указав, какие папки почтового ящика содержат спам и полезную почту.

Для того чтобы запустить Мастер обучения,

1. Откройте окно настройки приложения и выберите компонент **Анти-Спам** в разделе **Защита**.
2. Нажмите на кнопку **Мастер обучения** в правой части окна настройки.

Мастер обучения включает пошаговое выполнение процедуры обучения Анти-Спама. Переход к следующему шагу обучения осуществляется по кнопке **Далее**, возврат к предыдущему – по кнопке **Назад**.

Первым шагом Мастера обучения является выбор папок, содержащих полезную корреспонденцию. На данном этапе вам нужно выбрать лишь те папки, в чьем содержимом вы полностью уверены.

Вторым шагом Мастера обучения является выбор папок, содержащих спам. В случае если в вашем почтовом клиенте нет папок, содержащих нежелательные сообщения, пропустите данный шаг.

На третьем шаге выполняется автоматическое обучение Анти-Спама на выбранных вами папках. Почтовые сообщения этих папок пополняют базу Анти-Спама. Отправители полезной почты автоматически заносятся в «белый» список адресов.

На четвертом шаге необходимо сохранить результаты обучения одним из следующих способов: добавить результаты обучения к существующей базе Анти-Спама или заменить текущую базу на базу, полученную в результате обучения. Пожалуйста, помните, что для корректного распознавания спама необходимо произвести обучение как минимум на 50 письмах полезной почты и 50 письмах нежелательной корреспонденции. Без этого алгоритм iBayes работать не будет.

В целях экономии времени Мастер производит обучение только на 50 письмах в каждой выбранной папке.

13.2.2. Обучение на исходящих письмах

Вы можете включить обучение Анти-Спама на исходящих письмах вашего почтового клиента. В этом случае на основании анализа исходящих сообщений будет пополняться «белый» список адресов Анти-Спама. Для обучения используются только первые пятьдесят исходящих сообщений, затем обучение будет завершено.

Чтобы включить обучение Анти-Спама на исходящих сообщениях:

1. Откройте окно настройки приложения и выберите компонент **Анти-Спам** в разделе **Защита**.
2. Установите флажок ☑ **Обучаться на исходящих письмах** в разделе **Обучение**.

Внимание!

Обучение Анти-Спама на исходящих сообщениях, отправляемых по протоколу MAPI, происходит только в случае установленного флажка **Проверять при отправке** в модуле расширения Почтового Антивируса для Microsoft Office Outlook (см. п. 13.3.8 на стр. 198).

13.2.3. Обучение с использованием вашего почтового клиента

Обучение в процессе непосредственной работы с электронной корреспонденцией предполагает использование специальных кнопок в панели инструментов вашего почтового клиента.

При установке на компьютер Анти-Спам встраивается в следующие почтовые клиенты:

- Microsoft Office Outlook.
- Microsoft Outlook Express (Windows Mail).
- The Bat!

В результате в панели задач почтового клиента Microsoft Office Outlook появляются две кнопки **Спам** и **Не Спам** и закладка **Анти-Спам** с действиями в меню **Сервис → Параметры** (см. п. 13.3.8 на стр. 198). В Microsoft Outlook Express, помимо кнопок **Спам** и **Не Спам**, в панели задач добавляется кнопка **Настройка**, по которой открывается окно с действиями над нежелательной почтой (см. п. 13.3.9 на стр. 201). В почтовом клиенте The Bat! данные кнопки отсутствуют, однако для обучения вы можете воспользоваться специальными пунктами **Пометить как спам** и **Пометить как НЕ спам** в меню **Специальное**.

Если вы считаете, что выбранное письмо является спамом, нажмите на кнопку **Спам**. Если письмо не является спамом, нажмите на кнопку **Не Спам**. После этого Анти-Спам проводит обучение на выбранном письме. Если вы выделяете несколько писем, то обучение происходит на всех выделенных письмах.

Внимание!

В случае, когда вы вынуждены выделять сразу несколько писем либо уверены, что некоторая папка содержит письма только одной группы (спам или не спам), возможен пакетный подход к обучению компонента с помощью Мастера обучения (см. п. 13.2.1 на стр. 182).

13.2.4. Обучение с использованием отчетов Анти-Спама

Предусмотрена возможность проводить обучение Анти-Спама, основываясь на его отчетах.

Для того чтобы просмотреть отчеты компонента,

1. Выберите компонент **Анти-Спам** в разделе **Защита** главного окна приложения.
2. Щелкните левой клавишей мыши в блоке **Статистика**.

Отчеты компонента позволяют сделать вывод о точности его настройки и, при необходимости, внести определенные коррективы в работу Анти-Спама.

Для того чтобы отметить некоторое письмо как спам или не спам,

1. Выберите его в списке отчета на закладке **События** и воспользуйтесь кнопкой **Действия**.
2. Выберите один из следующих пунктов (см. рис. 53):
   - **Отметить как спам**.
   - **Отметить как не спам**.
   - **Добавить в «белый» список**
   - **Добавить в «черный» список**

Анти-Спам произведет дополнительное обучение на основании данного письма.

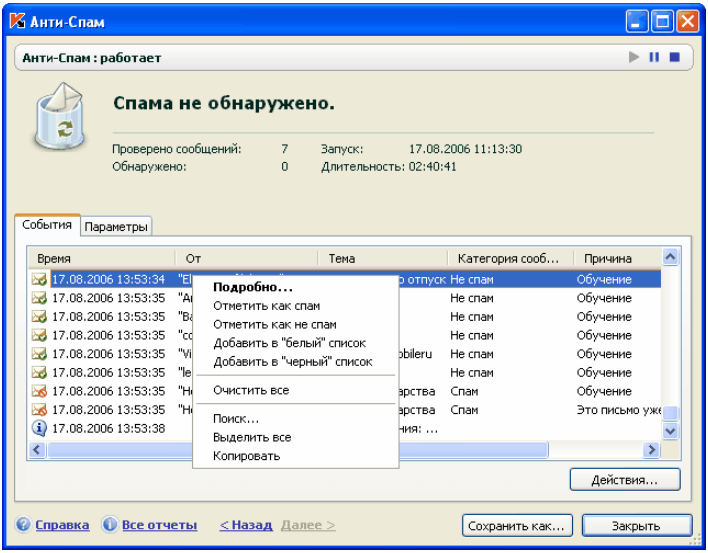


Рисунок 53. Обучение Анти-Спама на собственных отчетах

13.3. Настройка Анти-Спама

Неотъемлемым атрибутом защиты от спама является тонкая настройка Анти-Спама. Все параметры работы компонента размещены в окне настройки Антивируса Касперского и позволяют вам:

- Определять особенности работы компонента Анти-Спам (см. п. 13.3.1 на стр. 187).
- Выбирать использование различных технологий фильтрации спама (см. п. 13.3.2 на стр. 188).
- Регулировать точность определения спама и потенциального спама (см. п. 13.3.3 на стр. 189).
- Сформировать «черный» и «белый» списки для отправителей и ключевых фраз (см. п. 13.3.4 на стр. 190).
- Настроить дополнительные признаки фильтрации спама (см. п. 13.3.5 на стр. 195).
- Максимально снизить объем спама в вашем почтовом ящике за счет предварительной работы в Диспетчере Писем (см. п. 13.3.6 на стр. 196).

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

13.3.1. Настройка параметров проверки

В качестве параметров проверки вы можете настроить:

- Следует ли проверять почтовый трафик протоколов POP3 и IMAP. Антивирус Касперского по умолчанию проверяет почту всех этих протоколов.
- Следует ли активировать модули расширения (плагины) для почтовых клиентов Microsoft Office Outlook, Outlook Express (Windows Mail) и The Bat!
- Следует ли каждый раз перед загрузкой почты по протоколу POP3 с почтового сервера в почтовый ящик пользователя предварительно просматривать ее в Диспетчере Писем (см. п. 13.3.6 на стр. 196).

Чтобы настроить перечисленные выше параметры,

1. Откройте окно настройки приложения и выберите компонент **Анти-Спам** в разделе **Защита**.
2. Установите соответствующие флажки в блоке **Встраивание в систему** (см. рис. 54).
3. Скорректируйте, если это необходимо, параметры сети.

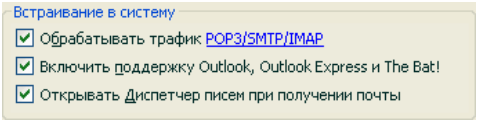


Рисунок 54. Настройка параметров проверки

Внимание! Если в качестве почтового клиента вы используете Microsoft Outlook Express, то при изменении статуса флажка **Включить поддержку Outlook, Outlook Express и The Bat!** требуется перезапускать почтовое приложение.

13.3.2. Выбор технологии фильтрации спама

Анализ почтовых сообщений на предмет спама осуществляется на основе использования современных технологий фильтрации:

- **Технология iBayes**, основанная на теореме Байеса, позволяет проводить анализ текста почтового сообщения на предмет обнаружения в нем фраз, относящихся к спаму. Анализ строится на основе статистики, полученной в результате обучения Анти-Спама (см. п. 13.2 на стр. 182).
- **Технология GSG**, позволяющая анализировать графические элементы электронного сообщения, используя уникальные графические сигнатуры для распознавания спама в виде изображений.
- **Технология PDB**, позволяющая анализировать заголовки электронного сообщения и классифицировать его как спам на основании набора эвристических правил.

По умолчанию включено использование всех технологий фильтрации, что позволяет максимально полно проводить анализ почтового сообщения на спам.

Чтобы отключить использование какой-либо технологии фильтрации:

1. Откройте окно настройки приложения и выберите компонент **Анти-Спам** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в блоке **Уровень агрессивности** и в открывшемся окне перейдите на закладку **Распознавание спама** (см. рис. 55).
3. Снимите флажки напротив технологий фильтрации, которые вы не хотите использовать при анализе почтовых сообщений на спам.

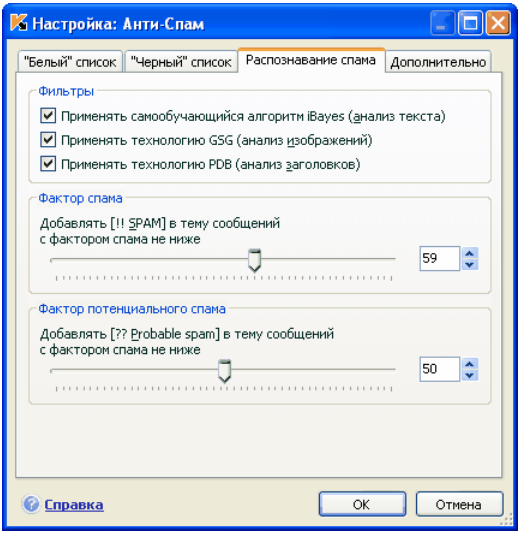


Рисунок 55. Настройка распознавания спама

13.3.3. Определение фактора спама и потенциального спама

Специалисты «Лаборатории Касперского» постарались максимально полно настроить Анти-Спам на опознавание спама и потенциального спама.

Распознавание спама основано на использовании современных технологий фильтрации (см. п. 13.3.2 на стр. 188), позволяющих на определенном количестве писем вашего почтового ящика достаточно точно обучить Анти-Спам распознавать спам, потенциальный спам и полезную почту.

Обучение Анти-Спама производится при работе Мастера обучения, при обучении из почтовых клиентов. При этом каждому отдельному элементу полезной почты или спама присваивается некоторый коэффициент. Когда в ваш почтовый ящик поступает почтовое сообщение, по технологии iBayes Анти-Спам проверяет письмо на наличие элементов спама и полезной почты. Коэффициенты каждого элемента спама (полезной почты) суммируются, и вычисляется *фактор спама* и *фактор потенциального спама*.

Фактор потенциального спама определяет вероятность, с которой письмо классифицируется как потенциальный спам. В случае использования **Рекомендуемого** уровня любое письмо с вероятностью более 50% и менее 59% будет считаться *потенциальным спамом*. Полезной почтой будет считаться почта, при проверке которой вероятность будет менее 50%.

Фактор спама определяет вероятность, с которой Анти-Спам относит почтовое сообщение к спаму. Любое письмо с вероятностью больше указанной, будет восприниматься как спам. По умолчанию для **Рекомендуемого** уровня фактор спама равен 59%. Это значит, что любое письмо с вероятностью более 59% будет отмечено как *спам*.

Всего предусмотрено пять уровней агрессивности (см. п. 13.1 на стр. 180), три из которых (**Высокий**, **Рекомендуемый** и **Низкий**) основываются на разных значениях факторов спама и потенциального спама.

Вы можете самостоятельно откорректировать алгоритм работы Анти-Спама. Для этого:

1. Откройте окно настройки приложения и выберите компонент **Анти-Спам** в разделе **Защита**.
2. В блоке **Уровень агрессивности** правой части окна нажмите на кнопку **Настройка**.
3. В открывшемся окне на закладке **Распознавание спама** (см. рис. 55) отрегулируйте факторы спама и потенциального спама в одноименных блоках.

13.3.4. Формирование «черного» и «белого» списков вручную

«Черный» и «белый» списки создаются пользователем вручную на основе работы компонента Анти-Спам с почтовой корреспонденцией. В эти списки заносится информация об адресах пользователей, письма с которых считаются заведомо полезными или, наоборот, спамом, а также различные характерные строки, ключевые слова, на основании которых сообщение идентифицируется как полезное или как спам.

Основное применение списков ключевых строк и, в частности, «белого» списка заключается в том, что вы можете договориться с доверенными адресатами, например, с вашими коллегами о том, чтобы «подписывать» вашу корреспонденцию некоторой строкой. Строка может быть любой. В качестве строки «подписи» вы можете использовать, например, PGP подпись. Как в подписи, так и в адресах допускается использование шаблонных символов: ***** и **?**. Под символом ***** подразумевается любая последовательность символов произвольной длины; под символом **?** – любой одиночный символ.

Если символы ***** и **?** входят в состав подписи, чтобы не возникло ошибки их восприятия Анти-Спамом, следует использовать предшествующий отменяющий символ **** . В этом случае вместо одного символа используются два: ***** и **\?**.

13.3.4.1. «Белый» список адресов и строк

В «белом» списке хранятся ключевые фразы писем, которые вы отметили как *не спам*, и адреса их отправителей, от которых, как вы считаете, спама приходить не должно. Заполнение «белого» списка строк выполняется вручную, а списка адресов отправителей – автоматически во время обучения компонента Анти-Спам. Вы можете откорректировать данный список.

Чтобы перейти к настройке «белого» списка,

1. Откройте окно настройки приложения и выберите компонент **Анти-Спам** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в правой части окна настройки.
3. Откройте закладку **«Белый» список** (см. рис. 56).

Закладка разделена на два блока: в верхнем блоке приводятся адреса отправителей полезной почты, в нижнем – ключевые фразы таких сообщений.

Чтобы включить использование «белых» списков фраз и адресов при фильтрации спама, установите соответствующие флажки в блоках **Разрешенные отправители** и **Разрешенные фразы**.

Посредством кнопок каждого из блоков вы можете редактировать списки.

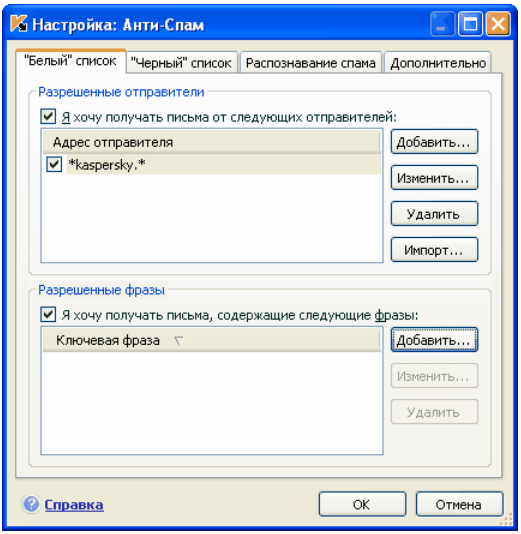


Рисунок 56. Настройка «белого» списка адресов и фраз

В качестве адреса списка вы можете задавать как адреса, так и маски адресов. При вводе адреса регистр не учитывается. Рассмотрим примеры масок адресов:

- *ivanov@test.ru* – почтовые сообщения от отправителя с таким адресом всегда классифицируются как полезная почта;
- **@test.ru* – почта от любого отправителя почтового домена *test.ru* является полезной; например: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@** – отправитель с таким именем, независимо от почтового домена, всегда отправляет только полезную почту; например: *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test** – почта любого отправителя почтового домена, начинающегося с *test*, не является спамом; например: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.*@test.???* – почта от отправителя, имя которого начинается на *ivan.* и имя почтового домена которого начинается на *test* и оканчивается на последние три любых символа, всегда является полезной; например: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

В качестве строки можно также использовать маски. При вводе строки регистр не учитывается. Вот примеры некоторых из них:

- *Привет, Иван!* – письмо, содержащее только этот текст, является полезным. Не рекомендуется использовать подобного рода строки в качестве строки «белого» списка.
- *Привет, Иван!** – письмо, начинающееся со строки *Привет, Иван!*, является полезным.
- *Привет, *! ** – почтовое сообщение, начинающееся с приветственного слова *Привет* и восклицательного знака в любом месте письма, не является спамом.
- ** Иван? ** – письмо содержит обращение к пользователю с именем *Иван*, после имени которого идет любой символ, и не является спамом.
- ** Иван\? ** – почтовое сообщение, содержащее строку *Иван?*, является полезным.

Если на данный момент времени вы хотите отменить классификацию некоторого адреса или фразы как атрибутов полезной почты, необязательно удалять их из списка, просто снимите флажки рядом с их названиями.

Для адресов «белого» списка предусмотрена возможность импорта из файла формата CSV.

13.3.4.2. «Черный» список адресов и строк

В «черном» списке отправителей хранятся ключевые фразы писем, которые, как вы считаете, являются *спамом*, и адреса их отправителей. Список заполняется вручную.

Чтобы перейти к заполнению «черного» списка,

1. Откройте окно настройки приложения и выберите компонент **Анти-Спам** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в правой части окна настройки.
3. Откройте закладку **«Черный» список** (см. рис. 57).

Закладка разделена на два блока: в верхнем блоке приводятся адреса отправителей спама, в нижнем – ключевые фразы таких сообщений.

Чтобы включить использование «черных» списков фраз и адресов при фильтрации спама, установите соответствующие флажки в блоках **Запрещенные отправители** и **Запрещенные фразы**.

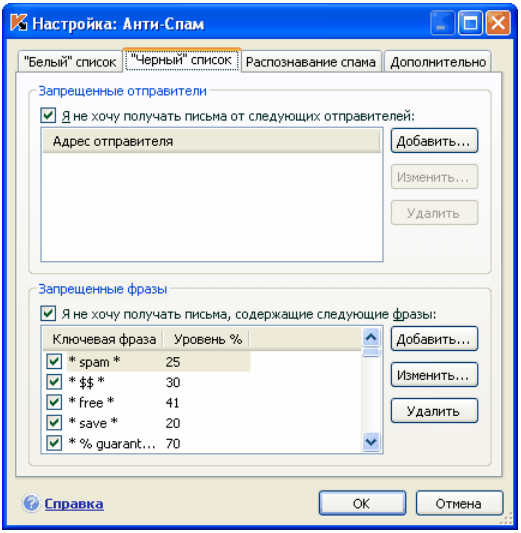


Рисунок 57. Настройка «черного» списка адресов и фраз

Посредством кнопок каждого из блоков вы можете редактировать списки.

В качестве адреса списка вы можете задавать как адреса, так и маски адресов. При вводе адреса регистр не учитывается. Рассмотрим примеры масок адресов:

- *ivanov@test.ru* – почтовые сообщения от отправителя с таким адресом всегда классифицируются как спам;
- **@test.ru* – почта от любого отправителя почтового домена *test.ru* является спамом; например: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@** – отправитель с таким именем, независимо от почтового домена, всегда отправляет только спам; например: *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test** – почта любого отправителя почтового домена, начинающегося с *test*, является спамом; например: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.*@test.???* – почта от отправителя, имя которого начинается на *ivan.* и имя почтового домена которого начинается на *test* и оканчивается на последние три любых символа, всегда является спамом; например: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

В качестве строки можно также использовать маски. При вводе строки регистр не учитывается. Вот примеры некоторых из них:

- *Привет, Иван!* – письмо, содержащее только этот текст, является спамом. Не рекомендуется использовать подобного рода строки в качестве строк списка.
- *Привет, Иван!** – письмо, начинающееся со строки *Привет, Иван!*, является спамом.
- *Привет, *! ** – почтовое сообщение, начинающееся с приветственного слова *Привет* и восклицательного знака в любом месте письма, является спамом.
- ** Иван? ** – письмо содержит обращение к пользователю с именем *Иван*, после имени которого идет любой символ, и является спамом.
- ** Иван\? ** – почтовое сообщение, содержащее строку *Иван?*, является спамом.

Если на данный момент времени вы хотите отменить классификацию некоторого адреса или фразы как неотъемлемых признаков спама, необязательно удалять их из списка, просто снимите флажки рядом с их названиями.

13.3.5. Дополнительные признаки фильтрации спама

Кроме основных признаков, на основании которых будет производиться фильтрация сообщений на спам (формирование «белого» и «черного» списков, анализ на фишинг, анализ с помощью технологий фильтрации), вы можете задать дополнительные признаки.

Чтобы настроить дополнительные признаки фильтрации почты на спам:

1. Откройте окно настройки приложения и выберите компонент **Анти-Спам** в разделе **Защита**.
2. Нажмите на кнопку **Настройка** в правой части окна настройки.
3. Откройте закладку **Дополнительно** (см. рис. 58).

На закладке представлен список признаков, на основании которых сообщению будет присвоен статус *спам* с той или иной степенью вероятности.

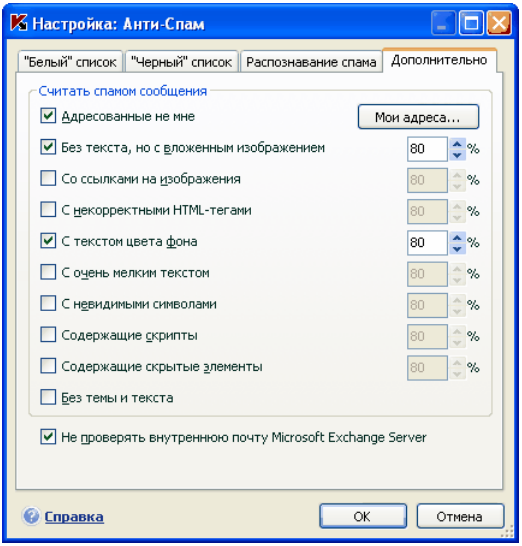


Рисунок 58. Дополнительные параметры распознавания спама

Чтобы включить использование какого-либо дополнительного признака фильтрации, установите напротив него флажок. Кроме того, для каждого из признаков требуется установить фактор спама (в процентах), который определяет вероятность, с которой письмо будет классифицировано как спам. По умолчанию фактор спама равен 80%. Сообщение будет отмечено как

спам, если сумма вероятностей по всем дополнительным признакам превысит 100%.

Спамом могут оказаться пустые сообщения (без темы и текста), сообщения содержащие ссылки на изображения или с вложенными изображениями, с текстом, совпадающим с цветом фона или с текстом, набранным мелким шрифтом. Также спамом могут быть письма с невидимыми символами (цвет текста совпадает с цветом фона), содержащие скрытые элементы (элементы не отображаются вообще) или некорректные html-теги, а также письма, содержащие скрипты (последовательности инструкций, выполняющихся при открытии письма пользователем).

Если вы включаете фильтрацию по признаку «сообщения, адресованные не мне», вам потребуется указать список ваших доверенных адресов в окне, открывающемся по кнопке **Мои адреса**. При анализе сообщения на спам адрес получателя будет проверен. В случае если адрес не совпадет ни с одним адресом из вашего списка, сообщению будет присвоен статус *спам*.

Формирование и редактирование списка адресов осуществляется в окне **Мои почтовые адреса** с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

Для исключения из проверки на спам почтовых сообщений, пересылаемых в рамках внутренней сети (например, корпоративная почта), установите флажок ☑ **Не проверять внутреннюю почту Microsoft Exchange Server**. Обратите внимание, что сообщения будут считаться внутренней почтой, если в качестве почтового клиента на всех компьютерах сети используется Microsoft Office Outlook, а почтовые ящики пользователей расположены на одном Exchange-сервере либо эти серверы должны соединяться X400-коннекторами. Для того чтобы Анти-Спам анализировал данные сообщения, флажок требуется снять.

13.3.6. Диспетчер писем

Внимание!

Диспетчер писем доступен только в случае, если вы принимаете почту по протоколу POP3.

Диспетчер писем предназначен для просмотра списка сообщений электронной почты на сервере, не загружая их на ваш компьютер. Это позволяет отказаться от приема некоторых сообщений, не только экономя ваше время и деньги при работе с электронной корреспонденцией, но и снижая вероятность загрузки спама и вирусов на ваш компьютер.

Диспетчер писем открывается в том случае, если в окне настройки компонента **Анти-Спам** установлен флажок ☑ **Открывать Диспетчер писем при получении почты**.

Для того чтобы удалить письма с сервера, не загружая их на ваш компьютер,

установите флажки слева от писем, подлежащих удалению, и нажмите на кнопку **Удалить**. Письма, подлежащие удалению, будут удалены с сервера. Остальная корреспонденция будет загружена на ваш компьютер после закрытия окна Диспетчера.

Иногда бывает сложно решить, стоит ли вам принимать некоторое электронное письмо, основываясь лишь на данных об отправителе и теме письма. В таких случаях Диспетчер писем предоставляет вам расширенную информацию о письме, загружая его заголовки.

Для того чтобы просмотреть заголовки письма,

выберите письмо в списке входящей корреспонденции. Заголовки письма будут отображены в нижней части формы.

Заголовки писем имеют незначительный объем, исчисляющийся десятками байт, и не могут содержать вредоносного кода.

Просмотр заголовков может пригодиться, например, в следующей ситуации: спамеры устанавливают на компьютер вашего коллеги вредоносную программу, которая рассылает спам от его имени, пользуясь контакт-листом его почтового клиента. Вероятность того, что вы находитесь в контакт-листе вашего коллеги, весьма высока; это несомненно приведет к тому, что ваш ящик электронной почты будет переполнен спамом от вашего коллеги. В данной ситуации невозможно определить, используя лишь адрес отправителя, отправлено письмо вашим коллегой или спамером. Используйте заголовки письма! Просмотрите внимательно, кем отправлено данное письмо, когда и каков его объем. Проследите путь следования письма от отправителя до вашего почтового сервера. Вся эта информация должна быть в заголовках письма. Примите решение, действительно ли необходимо загружать данное письмо с сервера или все-таки лучше удалить его.

Примечание.

Вы можете отсортировать письма по любой из колонок списка сообщений. Для того чтобы применить сортировку, нажмите на заголовок колонки. Строки будут отсортированы по возрастающей. Для того чтобы поменять направление сортировки, повторно нажмите на заголовок колонки.

13.3.7. Действия над нежелательной почтой

Если в результате проверки выясняется, что письмо является спамом или потенциальным спамом, дальнейшие операции Анти-Спама зависят от ста-

туса объекта и выбранного действия. По умолчанию электронные сообщения, являющиеся *спамом* или *потенциальным спамом*, модифицируются: в поле **Тема** письма добавляется метка **[!! SPAM]** или **[?? Probable Spam]**, соответственно.

Вы можете выбрать дополнительные действия над спамом и потенциальным спамом. В почтовых клиентах Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail) и The Bat! для этого предусмотрены специальные модули расширения. Для других почтовых клиентов вы можете настроить правила фильтрации.

13.3.8. Настройка обработки спама в Microsoft Office Outlook

Обратите внимание, что в приложении, установленном на компьютере под управлением Microsoft Windows 9x, плагин проверки почтовой корреспонденции на спам для Microsoft Office Outlook отсутствует.

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как *спам* или *потенциальный спам*, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**.

Дополнительные действия над спамом и потенциальным спамом в Microsoft Office Outlook приведены на специальной закладке **Анти-Спам** в меню **Сервис → Параметры** (см. рис. 59).

Она открывается автоматически при первой загрузке почтового клиента после установки приложения и предлагает вам настроить обработку нежелательной корреспонденции.

Как для спама, так и для потенциального спама вы можете задать следующие правила обработки:

Поместить в папку – нежелательная почта перемещается в указанную вами папку почтового ящика.

Скопировать в папку – создается копия почтового сообщения и помещается в указанную папку. Оригинальное письмо остается в папке **Входящие**.

Удалить – удалить нежелательную почту из почтового ящика пользователя

Пропустить – оставить почтовое сообщение в папке **Входящие**.

Для этого в блоке **Спам** или **Потенциальный спам** выберите соответствующее значение из раскрывающегося списка.

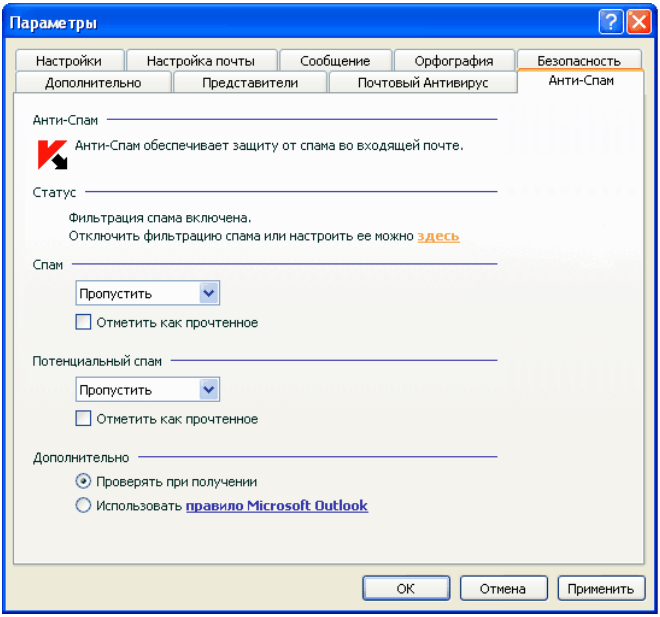


Рисунок 59. Детальная настройка обработки спама в Microsoft Office Outlook

Также вы можете указать алгоритм совместной работы программы Microsoft Office Outlook и плагина Анти-Спама:

- **Проверять при получении**. Все сообщения, поступающие в почтовый ящик пользователя, сначала обрабатываются в соответствии с настроенными правилами Microsoft Office Outlook. По завершении этой обработки оставшиеся сообщения, не подпадающие ни под одно правило, передаются на обработку модулю расширения Анти-Спама. То есть обработка сообщений происходит в соответствии с очередностью. Иногда эта очередность может нарушаться, например, при одновременном поступлении большого количества писем в почтовый ящик. В результате этого могут возникать ситуации, что информация о письме, обработанном правилом Microsoft Office Outlook, заносится в отчет Анти-Спама со статусом *спам*. Во избежание этого мы рекомендуем настроить работу плагина Анти-Спама в качестве правила Microsoft Office Outlook.
- **Использовать правило Microsoft Office Outlook**. В данном случае обработка сообщений, поступающих в почтовый ящик пользователя, осуществляется на основе иерархии сформированных правил программы Microsoft Office Outlook. В качестве одного из правил должно быть создано правило обработки сообщений Анти-Спамом. Это оптимальный алгоритм работы, при котором не возникает конфликтов между программами Microsoft Office Outlook и модулем расширения Анти-Спама.

Единственный недостаток данного алгоритма: создание и удаление правила обработки сообщений на спам через программу Microsoft Office Outlook осуществляется вручную.

Использование модуля расширения Анти-Спама в качестве правила Microsoft Office Outlook не поддерживается в версии Microsoft Office XP, установленной под операционной системой Microsoft Windows 9x/ME/NT4.0, из-за ошибки в программе Microsoft Office Outlook XP.

Чтобы создать правило обработки сообщений на спам:

1. Запустите программу Microsoft Office Outlook и воспользуйтесь командой **Сервис → Правила и оповещения** главного меню программы. Команда вызова мастера зависит от вашей версии Microsoft Office Outlook. В данном Руководстве приведено описание создания правила с помощью Microsoft Office Outlook 2003.

2. В окне **Правила и оповещения** перейдите на закладку **Правила для электронной почты** и нажмите на кнопку **Новое**. В результате будет запущен мастер создания нового правила. Его работа состоит из последовательности окон/шагов:

   шаг первый

   Вам предлагается выбрать создание правила «с нуля» либо по шаблону. Выберите вариант **Создать новое правило** и в качестве условия проверки выберите **Проверка сообщений после получения**. Нажмите на кнопку **Далее**.

   шаг второй

   В окне выбора условий отбора сообщений, не устанавливая флажков, нажмите на кнопку **Далее**. Подтвердите применение данного правила ко всем получаемым сообщениям в окне запроса подтверждения.

   шаг третий

   В окне выбора действий над сообщениями установите в списке действий флажок  **выполнить дополнительное действие**. В нижней части окна нажмите на ссылку дополнительное действие. И в открывшемся окне выберите из раскрывающегося списка **Kaspersky Anti-Spam**, нажмите на кнопку **ОК**.

   шаг четвертый

   В окне выбора исключений из правила, не устанавливая флажков, нажмите на кнопку **Далее**.

шаг пятый

В окне завершения создания правила вы можете изменить его имя (по умолчанию установлено **Kaspersky Anti-Spam**). Проверьте, что флажок **Включить правило** установлен и нажмите на кнопку **Готово**.

3. Новое правило по умолчанию будет добавлено первым в список правил окна **Правила и оповещения**. Переместите это правило в конец списка, если хотите, чтобы оно применялось к сообщению последним.

Все сообщения, поступающие в почтовый ящик, обрабатываются на основе правил. Очередность применения правил зависит от приоритета, который задан каждому правилу. Правила начинают применяться с начала списка, каждое последующее правило имеет приоритет ниже, чем предыдущее. Вы можете понижать или повышать приоритет применения правил к сообщению.

Если вы не хотите, чтобы после выполнения какого-либо правила сообщение дополнительно обрабатывалось правилом Анти-Спама, требуется в параметрах этого правила установить флажок **остановить дальнейшую обработку правил** (см. шаг третий окна создания правил).

Если вы имеете опыт создания правил обработки электронных сообщений в Microsoft Office Outlook, вы можете создать собственное правило для Анти-Спама на основе предложенного выше алгоритма.

13.3.9. Настройка обработки спама в Microsoft Outlook Express (Windows Mail)

При включении/ выключении плагина для Microsoft Outlook Express требуется выполнять перезапуск почтового приложения.

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как *спам* или *потенциальный спам*, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**.

Дополнительные действия над спамом и потенциальным спамом в Microsoft Outlook Express (Windows Mail) приведены в специальном окне (см. рис. 60), которое открывается по кнопке **Настройка**, расположенной рядом с другими кнопками Анти-Спама в панели задач: **Спам** и **Не Спам**.

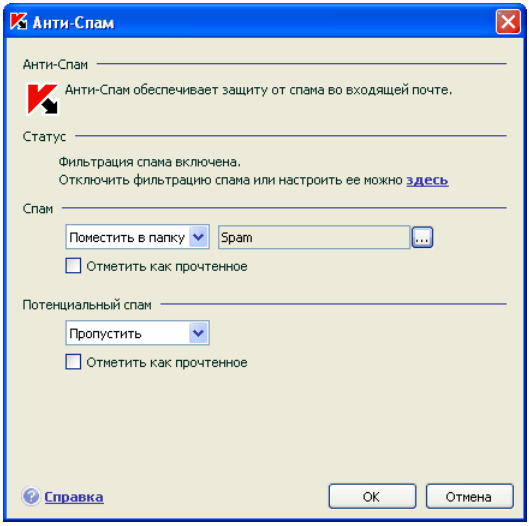


Рисунок 60. Детальная настройка обработки спама в Microsoft Outlook Express

Окно открывается автоматически при первой загрузке почтового клиента после установки приложения и предлагает вам настроить обработку нежелательной корреспонденции.

Как для спама, так и для потенциального спама вы можете задать следующие правила обработки:

Поместить в папку – нежелательная почта перемещается в указанную вами папку почтового ящика.

Скопировать в папку – создается копия почтового сообщения и помещается в указанную папку. Оригинальное письмо остается в папке **Входящие**.

Удалить – удалить нежелательную почту из почтового ящика пользователя

Пропустить – оставить почтовое сообщение в папке **Входящие**.

Для этого в блоке **Спам** или **Потенциальный спам** выберите соответствующее значение из раскрывающегося списка.

13.3.10. Настройка обработки спама в The Bat!

Действия над спамом и потенциальным спамом в почтовом клиенте The Bat! определяются средствами самого клиента.

Для того чтобы перейти к настройке правил обработки спама в The Bat!,

1. В меню **Свойства** почтового клиента выберите пункт **Настройка**.
2. В дереве настройки выберите пункт **Защита от спама** (см. рис. 61).

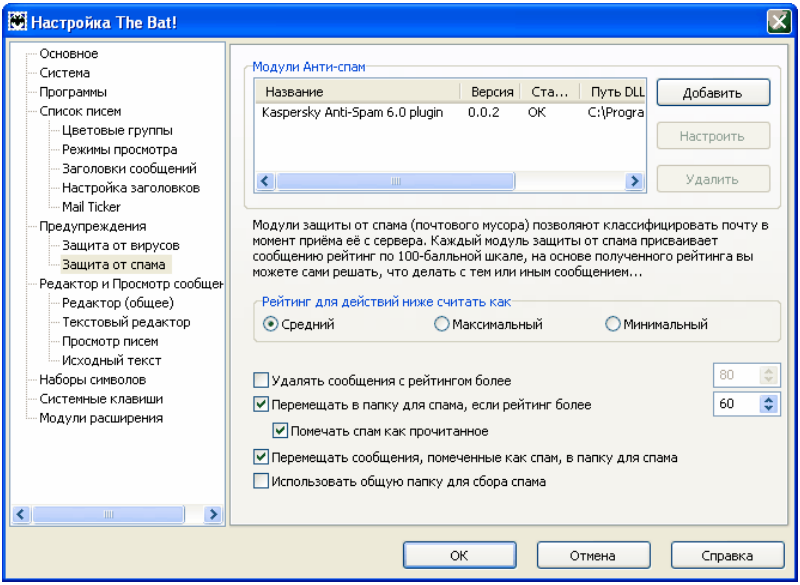


Рисунок 61. Настройка распознавания и обработки спама в The Bat!

Представленные параметры защиты от спама распространяются на все установленные на компьютере анти-спам-модули, поддерживающие работу с The Bat!

Вам нужно определить уровень рейтинга и указать, как поступать с сообщениями определенного рейтинга (в случае Анти-Спама – вероятности того, что письмо является спамом):

- Удалять сообщения с рейтингом более указанной величины.

- Перемещать сообщения с определенным рейтингом в специальную папку для спам-сообщений.
- Перемещать спам-сообщения, отмеченные специальным заголовком, в папку спама.
- Оставлять спам-сообщения в папке **Входящие**.

Внимание!

В результате обработки почтового сообщения Антивирус Касперского присваивает статус спама и потенциального спама письму на основании фактора (см. п. 13.3.3 на стр. 189), значение которого вы можете регулировать. В почтовом клиенте The Bat! реализован собственный алгоритм рейтинга сообщений на предмет спама, также основанный на факторе спама. Для того чтобы не было расхождений между фактором спама в Антивирусе Касперского и в The Bat!, все проверенные Анти-Спамом письма приводятся к рейтингу, соответствующему статусу письма: *полезная почта* – 0%, *потенциальный спам – 50 %*, спам – *100 %*.

Таким образом, рейтинг письма в почтовом клиенте The Bat! соответствует не фактору письма, заданному в Анти-Спаме, а фактору соответствующего статуса.

Подробнее о рейтинге спама и правилах обработки см. документацию к почтовому клиенту The Bat!

ГЛАВА 14. ПОИСК ВИРУСОВ НА КОМПЬЮТЕРЕ

Одной из важных составляющих обеспечения антивирусной защиты компьютера является поиск вирусов в указанных пользователем областях. Антивирус Касперского 6.0 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 защиты по тем или иным причинам.

В состав Антивируса Касперского 6.0 по умолчанию включены следующие задачи поиска вирусов:

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.

По умолчанию данные задачи выполняются с рекомендуемыми параметрами защиты. Вы можете изменять эти параметры (см. п. 14.4 на стр. 209), а также устанавливать расписание запуска задач (см. п. 6.5 на стр. 89).

Также предусмотрена возможность создавать собственные задачи (см. п. 14.3 на стр. 208) 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 6.0 или стандартными средствами

операционной системы Microsoft Windows (например, в окне программы **Проводник** или на **Рабочем столе** и т.д.).

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

14.1. Управление задачами поиска вирусов

Запуск задач проверки на вирусы осуществляется вручную или автоматически по сформированному расписанию (см. п. 6.5 на стр. 89).

Чтобы запустить задачу поиска вирусов вручную,

выберите имя задачи в разделе **Поиск вирусов** главного окна приложения и нажмите на кнопку ▶ в статусной строке.

Задачи, выполняющиеся в текущий момент (в том числе и задачи, сформированные через Kaspersky Administration Kit), отображаются в контекстном меню, открывающемся при нажатии правой кнопкой мыши по значку приложения в системной панели.

Чтобы приостановить задачу поиска вирусов,

в статусной строке нажмите на кнопку ⏸. При этом статус выполнения задачи изменится на *пауза*. Проверка будет приостановлена до того момента, пока задача не будет запущена снова вручную или по расписанию.

Чтобы остановить задачу поиска вирусов,

в статусной строке нажмите на кнопку ■. Статус выполнения задачи изменится на *прервано пользователем*. 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.

14.2. 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 под статусной строкой (см. рис. 62).

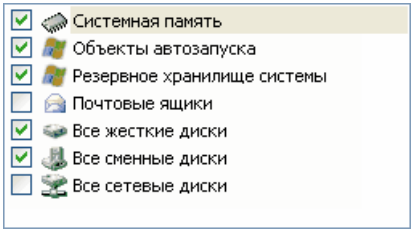


Рисунок 62. Список объектов для проверки

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 ящики пользователя, системная память, объекты автозапуска, резервное хранилище операционной системы, объекты, находящиеся в карантинном каталоге Антивируса Касперского.

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

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 нажмите на кнопку **Поиск вирусов** либо выберите пункт **Запуск** в меню, открывающемся при нажатии на кнопку **Действия**.

Кроме того, вы можете выбрать объект для проверки стандартными средствами операционной системы Microsoft Windows, например, в окне программы **Проводник** или на **Рабочем столе** и т.д. (см. рис. 63). Для этого установите курсор мыши на имени выбранного объекта, правой клавишей мыши откройте контекстное меню Microsoft Windows и выберите пункт **Проверить на вирусы**.

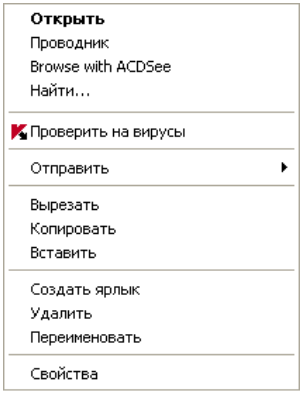


Рисунок 63. Проверка объекта из контекстного меню Microsoft Windows

14.3. 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 по правой клавише мыши или нажмите на кнопку **Действия**, расположенную справа от списка объектов проверки, и выберите пункт **Сохранить как**.
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. 14.2 на стр. 206), указать параметры, с которыми будет выполняться задача (см. п. 14.4 на стр. 209), а также, если требуется, настроить расписание (см. п. 6.5 на стр. 89) автоматического запуска.

Чтобы переименовать созданную задачу,

выберите задачу в разделе **Поиск вирусов** главного окна приложения, откройте контекстное меню по правой клавише мыши или нажмите на кнопку **Действия**, расположенную справа от списка объектов проверки, и выберите пункт **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, откройте контекстное меню по правой клавише мыши или нажмите на кнопку **Действия**, расположенную справа от списка объектов проверки, и выберите пункт **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.

14.4. 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 и выберите имя задачи в разделе **Поиск вирусов**.

В окне настройки для каждой из задач вы можете:

- выбрать уровень безопасности, на основе параметров которого будет выполняться задача (см. п. 14.4.1 на стр. 210);

- перейти к подробной настройке уровня:
    - указать параметры, определяющие типы файлов, подвергаемые анализу на вирусы (см. п. 14.4.2 на стр. 211);
    - настроить запуск задач от имени другой учетной записи (см. п. 6.4 на стр. 88);
    - указать дополнительные параметры проверки (см. п. 14.4.5 на стр. 217);
- восстановить параметры проверки, используемые по умолчанию (см. п. 14.4.3 на стр. 215);
- выбрать действие, которое будет применено приложением при обнаружении зараженного/ возможно зараженного объекта (см. п. 14.4.4 на стр. 215);
- сформировать расписание автоматического запуска задачи (см. п. 6.5 на стр. 89).
- Кроме того, вы можете установить единые параметры запуска для всех задач (см. п. 14.4.6 на стр. 219).

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

14.4.1. Выбор уровня безопасности

Каждая задача проверки на вирусы обеспечивает проверку объектов на одном из следующих уровней (см. рис. 64):

Высокий – 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 и при **Высоком** уровне, за исключением файлов почтовых форматов.

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

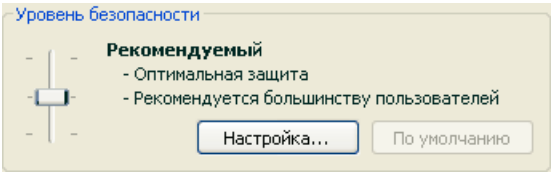


Рисунок 64. Выбор уровня безопасности при проверке объектов на вирусы

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 редактировать его параметры. В этом случае уровень станет **Пользовательским**.

Чтобы изменить параметры текущего уровня безопасности,

нажмите на кнопку **Настройка** в окне настройки задачи, в открывшемся окне отредактируйте параметры проверки объектов и нажмите на кнопку **ОК**.

В результате будет сформирован четвертый уровень безопасности – **Пользовательский** – содержащий параметры проверки, заданные вами.

14.4.2. 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. 65). 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.).

- **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. 330).

> 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 выберите 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.

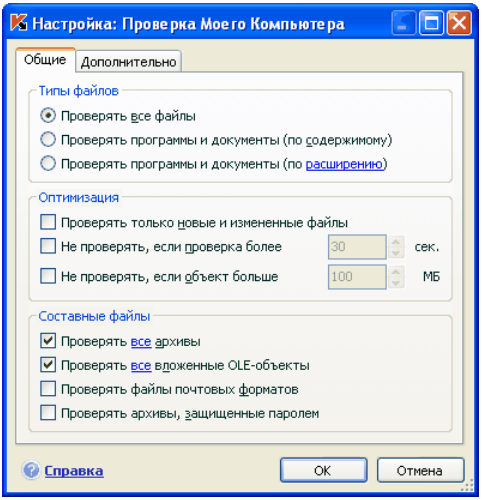


Рисунок 65. Настройка параметров проверки

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

- **Не проверять, если проверка 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, если объект больше…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.

14.4.3. 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. Выберите имя задачи в разделе **Поиск вирусов** главного окна и по ссылке Настройка перейдите в окно настройки параметров задачи.
2. Нажмите на кнопку **Восстановить** в разделе **Уровень безопасности**.

14.4.4. Выбор действия над объектами

Если в результате проверки объекта на вирусы выясняется, что он заражен или подозреваем 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,

выберите имя задачи в разделе **Поиск вирусов** главного окна приложения и по ссылке Настройка перейдите в окно настройки задачи. Все возможные действия приведены в соответствующем разделе (см. рис. 66).

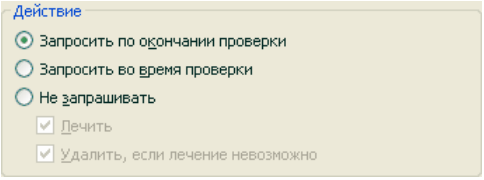


Рисунок 66. Выбор действия над опасным объектом

Если в качестве действия вы выбрали	При обнаружении зараженного/ возможно зараженного объекта
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.
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.
Не запрашивать	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.
Не запрашивать **Лечить**	Приложение, не запрашивая подтверждения пользователя, выполняет попытку лечения обнаруженного объекта. Если попытка лечения не удалась, объекту присваевается статус *возможно зараженный*, и он помещается на карантин (см. п. 17.1 на стр. 240). Информация об этом фиксируется в отчете (см. п. 17.3 на стр. 246). Позже можно попытаться вылечить этот

Если в качестве действия вы выбрали	При обнаружении зараженного/ возможно зараженного объекта
	объект.
Не запрашивать **Лечить** **Удалить, если лечение невозможно**	Приложение, не запрашивая подтверждения пользователя, выполняет попытку лечения обнаруженного объекта. Если попытка лечения объекта не удалась, он удаляется.
Не запрашивать **Лечить** **Удалить**	Приложение автоматически удаляет объект.

Перед лечением или удалением объекта Антивирус Касперского формирует его резервную копию и помещает ее в резервное хранилище (см. п. 17.2 на стр. 244) на тот случай, если понадобится восстановить объект или появится возможность его вылечить.

14.4.5. Дополнительные параметры поиска вирусов

Кроме настройки основных параметров проверки на вирусы вы можете установить дополнительные параметры (см. рис. 67):

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 сигнатур угроз, 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 сигнатуры угроз, архив будет проверен повторно.

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

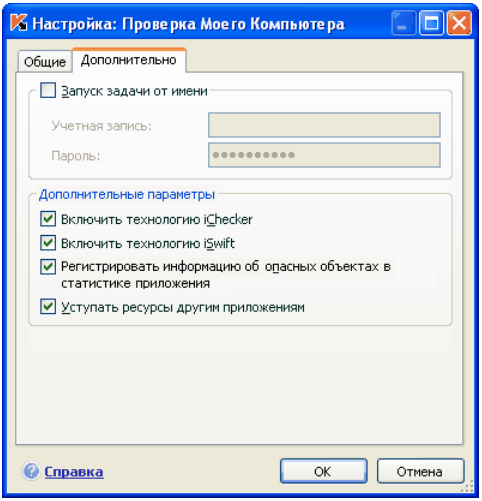


Рисунок 67. Дополнительная настройка проверки

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.

> Использование технологии iSwift недоступно на компьютерах с операционной системой Microsoft Windows 98SE/ME/XP64.

Регистрировать информацию об опасных объектах в статитстике приложения – сохранять информацию об обнаружении опасных объектов в общей статистике приложения, а также отображать список опасных угроз на закладке **Обнаружено** окна отчета (см. п. 17.3.2 на стр. 250). В случае если флажок снят, информация об опасных объектах не будет отбражаться в отчете, следовательно, обработать данные объекты будет невозможно.

Уступать ресурсы другим приложениям – приостанавливать выполнение данной задачи проверки на вирусы, если ресурсы процессора заняты другими приложениями.

14.4.6. 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. Выберите раздел **Поиск вирусов** в левой части главного окна приложения и воспользуйтесь ссылкой Настройка.
2. В открывшемся окне настройки установите параметры проверки: выберите уровень безопасности (см. п. 14.4.1 на стр. 210), произведите дополнительную настройку уровня, укажите действие над объектами (см. п. 14.4.4 на стр. 215).
3. Для применения установленных параметров ко всем задачам нажмите на кнопку **Применить** в разделе **Параметры других задач**. Подтвердите назначение единых параметров в окне запроса подтверждения.

ГЛАВА 15. 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.

15.1. Тестовый «вирус» EICAR и его модификации

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

Тестовый «вирус» НЕ ЯВЛЯЕТСЯ ВИРУСОМ и не содержит программного кода, который может 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 сигнатур угроз не содержат описания процедуры лечения данного объекта. Приложение перемещает объект на карантин для последующей обработки с обновленными сигнатурами угроз.
`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.

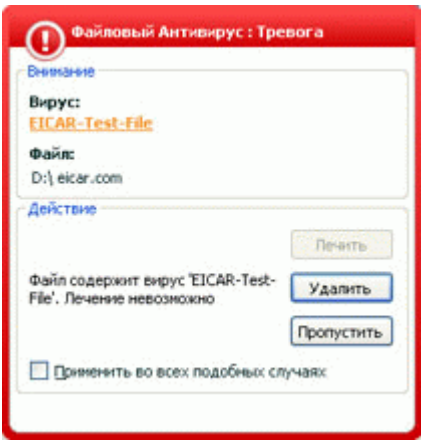
Действия над каждым из объектов определяются значениями параметров антивирусной проверки.

15.2. 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. 15.1 на стр. 220), 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 окне настройки отчетов.
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:



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.

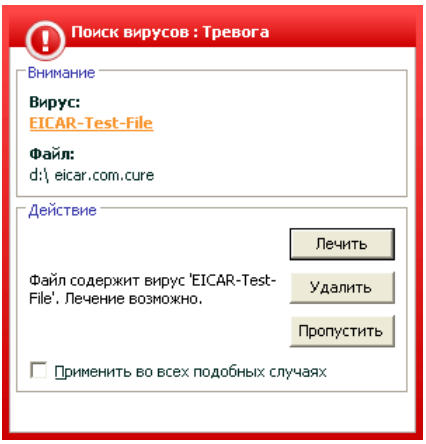
15.3. Проверка задачи Поиска вирусов

Для проверки задачи Поиска вирусов,

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации (см. п. 15.1 на стр. 220), а также созданные вами модификации тестового «вируса».
2. Создайте новую задачу (см. п. 14.3 на стр. 208) поиска вирусов и в качестве объекта проверки выберите папку, содержащую набор тестовых «вирусов» (см. п. 14.2 на стр. 206).
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 окне настройки отчетов.

4. Запустите задачу (см. п. 14.1 на стр. 206) 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:



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 16. 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:

- **Сигнатур угроз, сигнатур сетевых атак и сетевых драйверов**

  Защита информации на вашем компьютере обеспечивается на основании баз данных, содержащих сигнатуры угроз, описание сетевых атак. Компоненты защиты используют их при поиске опасных объектов на вашем компьютере и их обезвреживании. Сигнатуры ежечасно пополняются записями о новых угрозах и способах борьбы с ними. Поэтому настоятельно рекомендуется регулярно обновлять их.

  Кроме того, наряду с сигнатурами угроз и базой сетевых атак обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

  В предыдущих версиях антивирусных приложений «Лаборатории Касперского» поддерживалась работа с разными наборами антивирусных 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 антивирусных баз. Теперь при работе наших продуктов используются сигнатуры угроз, которые позволяют защищать не только от различных видов вредоносных и потенциально-опасных объектов, но и от хакерских атак.

- **Модулей приложения**

  Помимо сигнатур угроз вы можете обновлять и 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.

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, +7 (495) 956-70-00 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 Антивирус 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 сигнатуры угроз на вашем компьютере сравниваются с расположенными в источнике обновлений. В случае если на вашем компьютере установлена последняя версия сигнатур и модулей, на экран выдается информационное сообщение об актуальности защиты вашего компьютера. Если сигнатуры и модули отличаются, то на ваш компьютер будет установлена именно недостающая часть обновлений. Полное копирование сигнатур и модулей не производится, что позволяет существенно увеличить скорость обновления и заметно снизить объем трафика.

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

Возможность отката (см. п. 16.2 на стр. 227) необходима, например, в том случае, если вы обновили сигнатуры угроз и в процессе работы они повредились. Вы сможете вернуться к предыдущему варианту сигнатур, а позже попробовать обновить их еще раз.

Одновременно с обновлением приложения вы можете выполнять копирование полученных обновлений в локальный источник (см. п. 16.4.4 на стр. 236). Данный сервис позволяет обновлять базы данных и модули, используемые приложениями версии 6.0, на компьютерах сети в целях экономии интернет-трафика.

16.1. Запуск обновления

В любой момент вы можете запустить обновление приложения. Оно будет производиться из выбранного вами источника обновлений (см. п. 16.4.1 на стр. 229).

Запустить обновление приложения вы можете:

- из контекстного меню (см. п. 4.2 на стр. 55);
- из главного окна приложения (см. п. 4.3 на стр. 57).

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. Выберите компонент **Обновление** в разделе **Сервис**.
2. Нажмите на кнопку **Обновить** в правой части главного окна или на кнопку ▶ в статусной строке.

Процесс обновления приложения будет отражаться в специальном окне. Вы можете скрыть окно с текущими результатами обновления. Для этого нажмите на кнопку **Закрыть**. 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. 16.4.4 на стр. 236).

16.2. Откат последнего обновления

Каждый раз, когда вы запускаете обновление приложения, Антивирус Касперского сначала создает резервную копию текущих сигнатур угроз и только потом приступает к их обновлению. Это позволяет вам вернуться к использованию предыдущей версии сигнатур после неудачного обновления.

Чтобы вернуться к использованию предыдущей версии сигнатур угроз,

1. Выберите компонент **Обновление** в разделе **Сервис** главного окна приложения.
2. Нажмите на кнопку **Откатить** в правой части главного окна.

16.3. Создание задач обновления

Для обновления сигнатур угроз и модулей приложения в Антивирусе Касперского есть встроенная задача обновления. Однако вы можете создавать собственные задачи обновления с различными параметрами или расписанием запуска.

Например, вы установили Антивирус Касперского на мобильный компьютер, которым вы пользуетесь дома и в офисе. Дома обновление происходит с использованием серверов «Лаборатории Касперского», а в офисе – из локального каталога, содержащего необходимый набор обновлений. Чтобы каждый раз не изменять параметры обновления, специфичные для каждого из случаев, воспользуйтесь двумя различными задачами.

Чтобы создать дополнительную задачу обновления,

1. В разделе **Сервис** главного окна приложения выберите пункт **Обновление**, откройте контекстное меню по правой клавише мыши и выберите пункт **Сохранить как**.
2. В открывшемся окне введите имя задачи и нажмите на кнопку **ОК**. В результате задача с указанным именем появится в разделе **Сервис** главного окна приложения.

Внимание!

В Антивирусе Касперского действует ограничение на количество задач обновления, которые может создать пользователь. Максимальное количество: две задачи.

Новая задача наследует все параметры задачи, на основе которой она была создана, за исключением параметров расписания. По умолчанию автоматический запуск новой задачи отключен.

После создания задачи проведите дополнительную настройку: укажите источник обновления (см. п. 16.4.1 на стр. 229), параметры сетевого подключения (см. п. 16.4.3 на стр. 234), а также, если требуется, включите запуск задачи с правами (см. п. 6.4 на стр. 88) и настройте расписание (см. п. 6.5 на стр. 89).

Чтобы переименовать задачу,

выберите задачу в разделе **Сервис** главного окна приложения, откройте контекстное меню по правой клавише мыши и выберите пункт **Переименовать**.

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

Чтобы удалить задачу,

выберите задачу в разделе **Сервис** главного окна приложения, откройте контекстное меню по правой клавише мыши и выберите пункт **Удалить**.

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

Внимание!

Операции переименования и удаления доступны только для пользовательских задач.

16.4. Настройка обновления

Обновление приложения выполняется в строгом соответствии с параметрами, определяющими:

- с какого ресурса производится копирование и установка обновлений приложения (см. п. 16.4.1 на стр. 229);
- в каком режиме запускается процесс обновления приложения и что именно обновляется (см. п. 16.4.2 на стр. 232);
- как часто требуется запускать обновление, в случае если настроен запуск по расписанию (см. п. 6.5 на стр. 89);
- от имени какой учетной записи будет выполнено обновление (см. п. 6.4 на стр. 88);
- требуется ли копировать полученные обновления в локальный каталог (см. п. 16.4.4 на стр. 236);
- какие действия нужно выполнять после обновления приложения (см. п. 16.4.4 на стр. 236).

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

16.4.1. Выбор источника обновлений

Источник обновлений – это некоторый ресурс, содержащий обновления сигнатур угроз и модулей Антивируса Касперского.

В качестве источника обновления вы можете использовать:

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

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, +7 (495) 956-70-00 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 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 обновления производится на закладке **Источник обновления** (см. рис. 68).

По умолчанию обновление производится с серверов обновлений «Лаборатории Касперского». Список серверов не доступен для редактирования. В процессе обновления Антивируса 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.

Чтобы обновление производилось с некоторого ftp-, http-сайта,

1. Нажмите на кнопку **Добавить**.
2. Выберите ftp-, http-сайт в окне **Выбор источника обновления** или укажите его IP-адрес, символьное имя или url-адрес в поле **Источник**. При выборе в качестве источника обновления некоторого ftp-ресурса допускается указание параметров авторизации в

url-адресе сервера в формате ftp://<имя пользователя>:<пароль>@<хост>:<порт>.

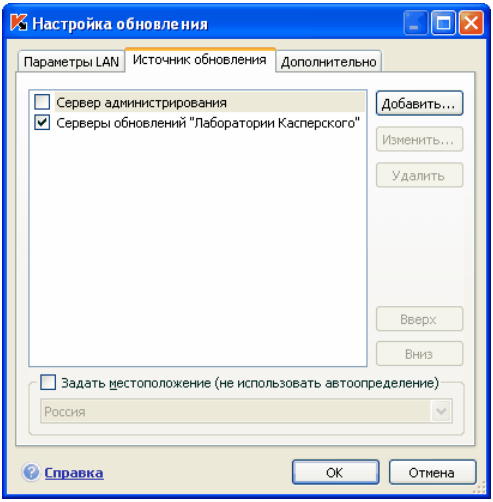


Рисунок 68. Выбор источника обновления

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 обновления** или введите полный путь к нему в поле **Источник**.

Антивирус Касперского добавляет новый источник обновления в начало списка и автоматически включает его использование – устанавливает рядом с ним флажок.

Если в качестве источников обновления 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.

16.4.2. Выбор режима и предмета обновления

Важным моментом в настройке обновления приложения является определение предмета обновления и режима обновления.

Предмет обновления (см. рис. 69) определяет, что именно будет обновляться:

- сигнатуры угроз;
- сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты;
- база сетевых атак, используемых в работе Анти-Хакера;
- модули приложения.

Сигнатуры угроз, сетевые драйверы и база сетевых атак обновляются всегда, а программные модули – только в том случае, если установлен соответствующий режим.

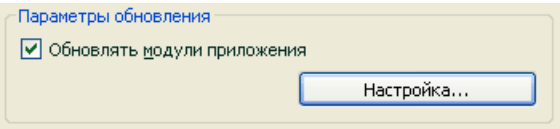


Рисунок 69. Выбор предмета обновления

Чтобы в процессе обновления на ваш компьютер копировались и устанавливались обновления модулей приложения,

установите флажок **Обновлять модули приложения** в окне настройки компонента **Обновление**.

Если на данный момент в источнике присутствует обновление модулей приложения, приложение получит необходимые обновления и применит их после перезагрузки компьютера. До перезагрузки полученные обновления модулей установлены не будут.

Если следующее обновление приложения происходит до перезагрузки компьютера и установки полученных ранее обновлений модулей приложения, то будет произведено только обновление сигнатур угроз.

Режим обновления приложения (см. рис. 70) 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 обновления. При обнаружении свежих обновлений Антивирус 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 сигнатур угроз, сетевых атак и модулей приложения, что исключит возможность проникновения опасных программ на ваш компьютер.

Рисунок 70. 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 каждые 2 часа. Чтобы сформировать другое расписание, нажмите на кнопку **Изменить** рядом с названием режима и в открывшемся

окне произведите соответствующие изменения (подробнее см. п. 6.5 на стр. 89).

Вручную. В этом случае вы самостоятельно запускаете обновление приложения. Антивирус Касперского обязательно уведомит вас о необходимости обновления:

- во-первых, над значком приложения в системной панели появится всплывающее сообщение соответствующего содержания (если включен сервис уведомлений) (см. п. 17.11.1 на стр. 277);
- во-вторых, второй индикатор на главном окне приложения сообщит о том, что защита на вашем компьютере устарела (см. п. 5.1.1 на стр. 62);
- в-третьих, в разделе комментариев и советов главного окна появится рекомендация по обновлению приложения (см. п. 4.3 на стр. 57).

16.4.3. Настройка параметров соединения

Если в качестве источника обновления вы выбрали серверы обновлений «Лаборатории Касперского» или некоторый ftp-, http-сайт, рекомендуем вам проверить параметры соединения с интернетом.

Все параметры сгруппированы на специальной закладке – **Параметры LAN** (см. рис. 71).

Параметр **Использовать пассивный режим FTP, если возможно** используется в том случае, если вы загружаете обновления с ftp-сервера, соединение с которым выполняется в пассивном режиме (например, через сетевой экран). Если используется активный режим работы с FTP, вы можете снять данный флажок.

В поле **Тайм-аут соединения (сек.)** задайте время, отведенное на соединение с сервером обновления. Если соединение не произошло, по истечении заданного 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.

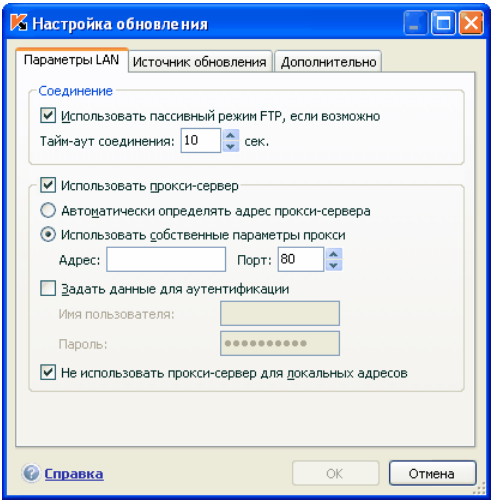


Рисунок 71. Настройка сетевых параметров обновления

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 для обновления приложения:

  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 удается, Антивирус Касперского использует параметры прокси-сервера, указанные в Microsoft Internet Explorer.

  Использовать собственные параметры прокси – 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.

- 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 **Задать данные для аутентификации** и укажите в приведенных ниже полях имя 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 запущено обновление (см. п. 6.4 на стр. 88).

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, при запуске обновления 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.

Для того чтобы при обновлении из локального или сетевого каталога не использовать прокси-сервер, установите флажок **Не использовать прокси-сервер для локальных адресов**.

Этот параметр недоступен в приложении, установленном на компьютере под управлением Microsoft Windows 9X/NT 4.0. Однако по умолчанию прокси-сервер для локальных адресов не используется.

16.4.4. Копирование обновлений

Сервис копирования обновлений предоставляет возможность оптимизировать нагрузку на сетевой трафик предприятия. Копирование обновлений выполняется в два этапа:

1. Один из компьютеров сети получает пакет обновлений приложения и сигнатур угроз 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. 72) 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, открывающемся по кнопке **Обзор**. Если флажок установлен, при получении новых обновлений они будут автоматически скопированы в данную папку.

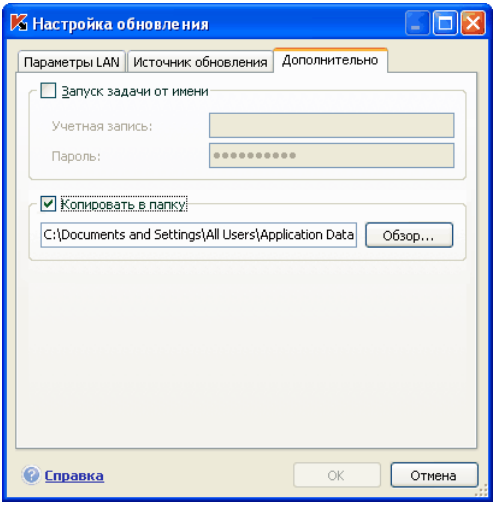


Рисунок 72. Настройка сервиса копирования обновлений

Обратите внимание, что Антивирус Касперского 6.0 получает с серверов «Лаборатории Касперского» только собственный пакет обновлений. Копирование обновлений для других приложений «Лаборатории Касперского» рекомендуется выполнять через Kaspersky Administration Kit.

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.

16.4.5. Действия после обновления приложения

Каждое обновление сигнатур угроз 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. 17.1 на стр. 240). Возможно после обновления сигнатур угроз Антивирус Касперского сможет однозначно определить опасность и обезвредить ее.

По умолчанию приложение проверяет объекты на карантине после каждого обновления сигнатур угроз. 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 14 на стр. 205). Рекомендуем настроить автоматический режим запуска данной задачи после каждого обновления сигнатур угроз (см. п. 6.5 на стр. 89).

ГЛАВА 17. 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. 17.2 на стр. 244). 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 сигнатур угроз (см. п. 17.1 на стр. 240).

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. 17.6 на стр. 265). Эксперты «Лаборатории Касперского» постарались включить все возможные способы обеспечения поддержки: онлайн-поддержка, форум вопросов и предложений от пользователей приложения и т.д.

- Сервис уведомлений о событиях помогает настраивать оповещение пользователей о важных моментах в работе Антивируса Касперского (см. п. 17.11.1 на стр. 277). 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. 17.11.2 на

стр. 280). Например, изменение уровня защиты может значительно повлиять на безопасность информации на вашем компьютере.

- Сервис управления лицензионными ключами позволяет получать подробную информацию об используемой лицензии, производить активацию вашей копии приложения, а также осуществлять управление файлами лицензионных ключей (см. п. 17.5 на стр. 262).

Также приложение предоставляет детальную справочную информацию (см. п. 17.4 на стр. 261) и подробные отчеты (см. п. 17.3 на стр. 246) 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. 17.7 на стр. 266).

Создание диска аварийного восстановления позволяет восстанавливать работоспособность компьютера на уровне, предшествующем заражению (см. п. 17.10 на стр. 272). 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. 17.9 на стр. 270).

Рассмотрим подробнее все перечисленные сервисы.

17.1. Карантин возможно зараженных объектов

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

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.

  Сигнатуры угроз содержат те угрозы, которые на настоящее время изучены специалистами «Лаборатории Касперского». Если вредоносная программа изменяется и в сигнатуры эти изменения еще не внесены, то Антивирус Касперского отнесет объект, пораженный из-

мененной 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 сигнатурах угроз 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, нажав на кнопку **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.

17.1.1. Действия с объектами на карантине

Общее количество объектов, помещенных на карантин, приводится в **Файлах данных** раздела **Сервис**. 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 кнопке **Очистить**. Обратите внимание, что при этом будут также удалены объекты резервного хранилища и файлы отчетов.

Чтобы перейти к объектам на карантине,

щелкните левой клавишей мыши в любой части блока **Карантин**.

На закладке карантина (см. рис. 73) 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.

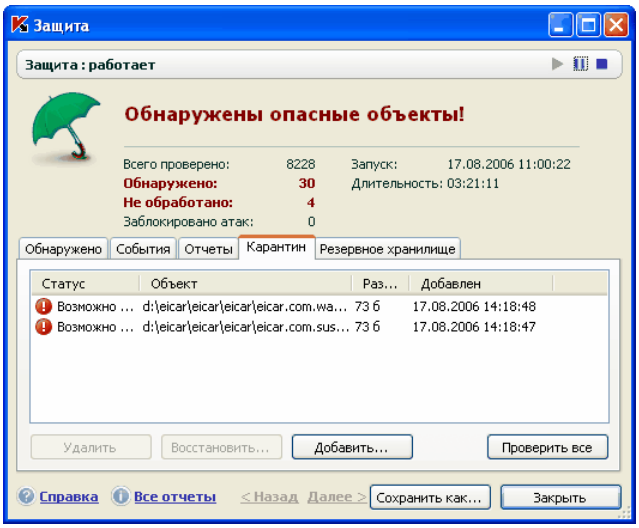


Рисунок 73. Список объектов на карантине

- Проверять и лечить с использованием текущей версии сигнатур угроз 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**.

17.1.2. Настройка параметров карантина

Вы можете настроить параметры формирования и работы карантина, а именно:

- Задать режим автоматической проверки объектов на карантине после каждого обновления сигнатур угроз (подробнее см. п. 16.4.4 на стр. 236).

  Внимание!

  Приложение не сможет проверить объекты карантина сразу после обновления сигнатур угроз, 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 Антивируса Касперского по ссылке Настройка из главного окна приложения.
2. Выберите **Файлы данных** в дереве настройки.
3. В блоке **Карантин и Резервное хранилище** (см. рис. 74) укажите временной период, после которого объекты, находящиеся в хранилище, будут автоматически удалены.

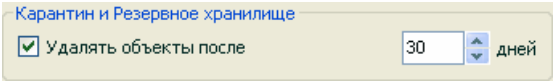


Рисунок 74. Настройка срока хранения объектов на карантине

17.2. 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.

17.2.1. Действия с резервными копиями

Общее количество резервных копий объектов, помещенных в хранилище, приводится в **Файлах данных** раздела **Сервис**. 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 кнопке **Очистить**. Обратите внимание, что при этом будут также удалены объекты карантина и файлы отчетов.

Чтобы перейти к копиям опасных объектов,

щелкните левой клавишей мыши в любой части блока **Резервное хранилище**.

В центральной части закладки (см. рис. 75) 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.

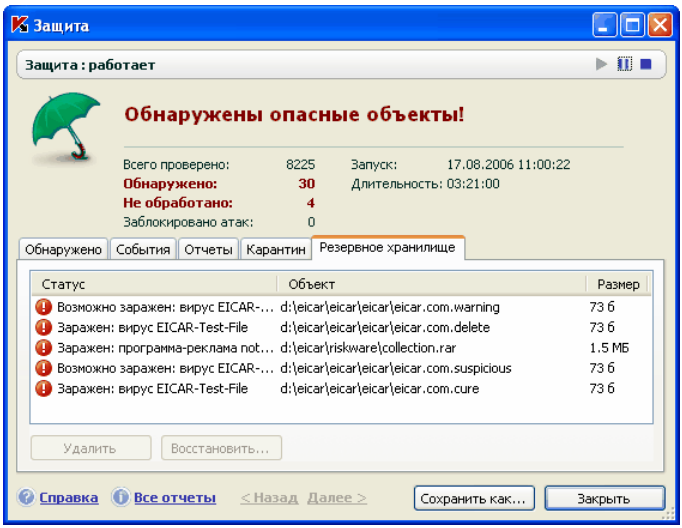


Рисунок 75. Резервные копии удаленных или вылеченных объектов

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 сигнатурами 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 удаляло наиболее старые копии из хранилища (см. п. 17.2.2 на стр. 246).

17.2.2. 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 Антивируса Касперского по ссылке Настройка из главного окна приложения.
2. Выберите **Файлы данных** в дереве настройки.
3. Настройте срок хранения резервных копий в хранилище в блоке **Карантин и Резервное хранилище** (см. рис. 74) правой части окна.

17.3. 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 в **Файлах данных** раздела **Сервис** главного окна приложения. Данная информация приведена в блоке **Отчеты**.

Чтобы перейти к просмотру отчетов,

щелкните левой клавишей мыши в любом месте блока **Отчеты**.

В результате будет открыто окно на закладке **Отчеты** (см. рис. 76). 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, *прервано* или *завершено*. Если вы хотите просмотреть пол-

ную историю формирования отчетов текущей сессии работы приложения, установите флажок **Показывать историю отчетов**.

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 **Подробно**.

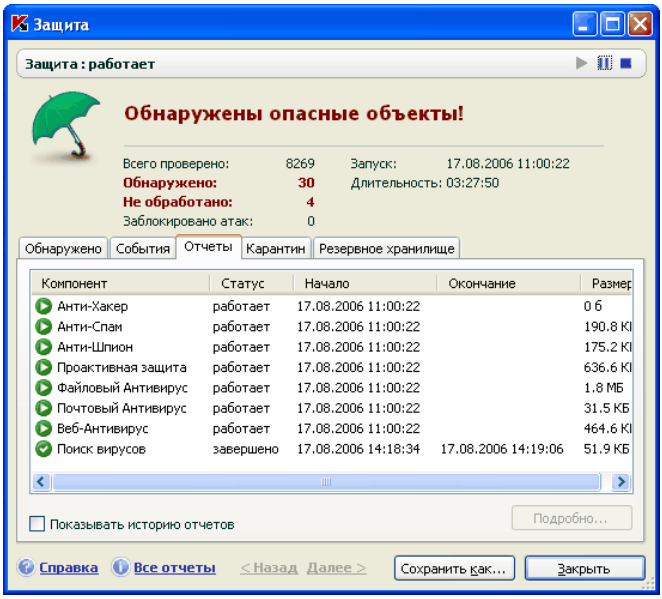


Рисунок 76. Отчеты о работе компонентов приложения

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 разный:

- 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 сигнатур угроз.

- Закладки **Макросы** и **Реестр** присутствуют только в отчете проактивной защиты и содержат информацию о всех макросах, попытка запуска которых была произведена на вашем компьютере, и о всех попытка изменения системного реестра операционной системы.

- Закладки **Фишинг-сайты**, **Всплывающие окна**, **Баннеры** и **Попытки автодозвона** включены только в отчет Анти-Шпиона. Они содержат информацию о всех обнаруженных попытках фишинг-атак, о всех заблокированных в текущем сеансе работы приложения всплывающих окнах, баннерах и попытках автоматического дозвона на платные ресурсы интернета.

- Закладки **Сетевые атаки**, **Заблокированные хосты**, **Активность приложений** и **Фильтрация пакетов** присутствуют только в отчете Анти-Хакера. Они включают информацию по всем сетевым атакам, попытка которых была произведена в отношении вашего компьютера, заблокированным в результате атак хостам; содержат описание сетевой активности приложений, подпадающей под созданные правила активности, и всех пакетов данных, удовлетворяющих правилам пакетной фильтрации Анти-Хакера.

- Закладки **Установленные соединения**, **Открытые порты** и **Трафик** также характеризуют сетевую активность на вашем компьютере, отображая текущие установленные соединения, открытые порты и объем переданного и полученного вашим компьютером сетевого трафика.

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 **Сохранить как** и укажите, куда бы вы хотели сохранить файл отчета.

По завершении работы с отчетом нажмите на кнопку **Закрыть**.

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 про-

сматриваете, список пунктов меню отличается, ниже приведены все возможные пункты):

Лечить – произвести попытку лечения опасного объекта. Если лечение будет успешно, объект будет восстановлен в исходное местоположение. Если обезвредить объект не получится, вы можете оставить его в этом списке для отложенной проверки с обновленными сигнатурами угроз или удалить. Вы можете применить данное действие как к одному объекту списка, так и к нескольким выбранным объектам.

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 сигнатур угроз.

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».

Посмотреть на www.google.com – найти информацию об объекте с помощью поисковой системы.

Поиск – задать условия поиска по имени объекта или статусу.

Кроме того, вы можете сортировать информацию, представленную в окне, по возрастанию и убыванию каждого из столбцов.

17.3.1. Настройка параметров отчетов

Для настройки параметров формирования и хранения отчетов:

1. Откройте окно настройки Антивируса Касперского по ссылке Настройка из главного окна приложения.
2. Выберите **Файлы данных** в дереве настройки.
3. В блоке **Отчеты** (см. рис. 77) 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 некритические 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 некритического характера.

- установите срок хранения отчетов. По умолчанию срок хранения отчетов составляет 30 дней, по истечении которого отчеты удаляются. Вы можете изменить максимальный срок хранения или отменить такое ограничение вообще.

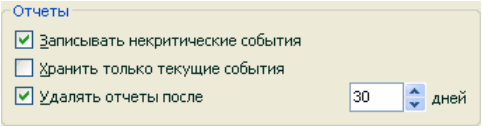


Рисунок 77. Настройка параметров формирования отчетов

17.3.2. Закладка *Обнаружено*

Данная закладка (см. рис. 78) 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**.

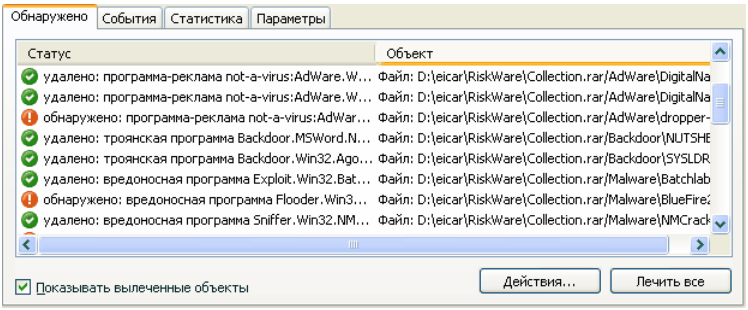


Рисунок 78. Список обнаруженных опасных объектов

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.

17.3.3. Закладка *События*

Полный список всех важных событий в работе компонента защиты или при выполнении задачи поиска вирусов либо обновления сигнатур угроз фиксируется на данной закладке (см. рис. 79), если это не было отменено правилом контроля активности (см. п. 10.1.1 на стр. 133).

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, *ok*, *не обработан*. Данные события отображаются в журнале событий только в том случае, если установлен флажок ☑ **Показывать все события**.

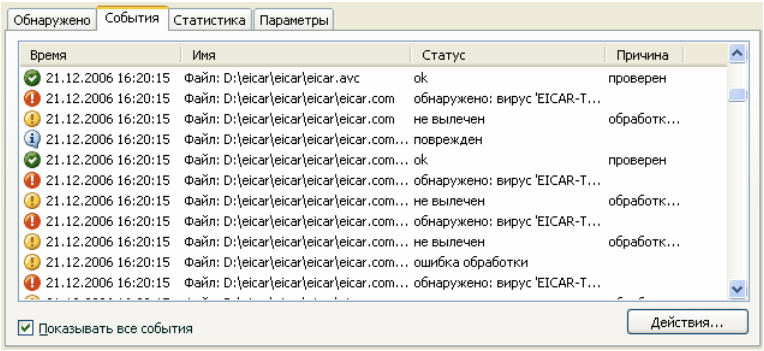


Рисунок 79. События, возникшие в работе компонента

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.

Вы также можете проводить обучение Анти-Спама с помощью специального контекстного меню при просмотре отчета данного компонента. Для этого выберите имя письма, по правой клавише мыши откройте контекстное меню и выберите **Отметить как спам**, если это письмо является спамом, или **Отметить как не спам**, если выбранное письмо – полезная почта. Кроме того, на основе информации, полученной при анализе письма, вы можете пополнить «белый» и «черный» списки Анти-Спама. Для этого воспользуйтесь соответствующими пунктами контекстного меню.

17.3.4. Закладка *Статистика*

Подробная статистика работы компонента или выполнения задачи поиска вирусов фиксируется на данной закладке (см. рис. 80). 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.

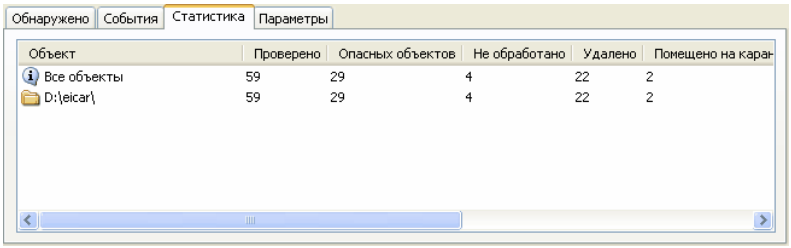


Рисунок 80. Статистика работы компонента

17.3.5. 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. 81). 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.

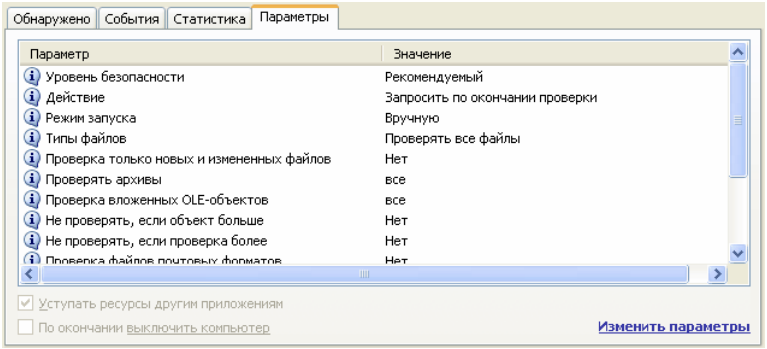


Рисунок 81. Параметры работы компонента

- 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 щелкайте 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.

17.3.6. Закладка *Макросы*

Все макросы, попытка выполнения которых была произведена в текущем сеансе работы Антивируса Касперского, приведены на закладке **Макросы** (см. рис. 82). Здесь приводится полное имя каждого макроса, время его исполнения и статус, отражающий результат обработки макроса.

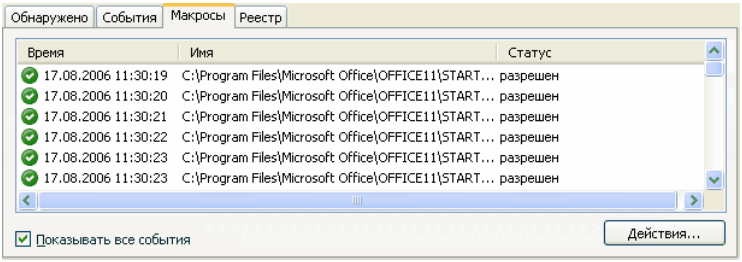


Рисунок 82. Список обнаруженных опасных макросов

Вы можете определить, какие события вы хотели бы видеть на этой закладке отчета. Чтобы отменить просмотр информационных событий, снимите флажок **Показывать все события**.

17.3.7. Закладка *Реестр*

Операции с ключами реестра, попытка которых была произведена с момента запуска приложения, фиксируются на закладке **Реестр** (см. рис. 83), если протоколирование не запрещено правилом (см. п. 10.1.3.2 на стр. 141).

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.

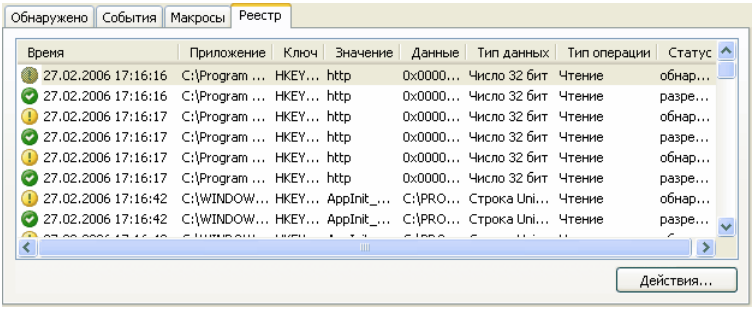


Рисунок 83. События по чтению и изменению системного реестра

17.3.8. Закладка *Фишинг-сайты*

Данная закладка отчета (см. рис. 84) отражает все попытки фишинг-атак, совершенные в текущем сеансе работы Антивируса Касперского. Указывается ссылка на фишинг-сайт, обнаруженная в письме, рассылке или присланная вам любым другим возможным способом, дата и время обнаружения атаки и статус атаки: была она заблокирована или нет.

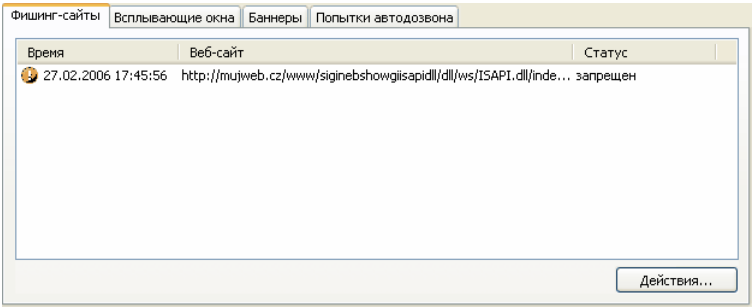


Рисунок 84. Попытки заблокированных фишинг-атак

17.3.9. Закладка *Всплывающие окна*

Адреса всех всплывающих окон, заблокированных Анти-Шпионом, приведены на данной закладке отчета (см. рис. 85). Такие окна, как правило, открываются на веб-сайтах в интернете.

Для каждого всплывающего окна фиксируется его адрес в интернете, дата и время, когда окно было заблокировано.

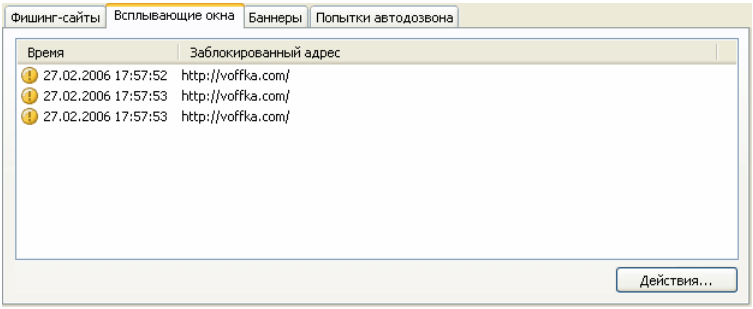


Рисунок 85. Список заблокированных всплывающих окон

17.3.10. Закладка *Баннеры*

Адреса обнаруженных в текущем сеансе работы Антивируса Касперского баннеров перечислены на этой закладке отчета (см. рис. 86). Каждый баннер характеризуется его адресом в интернете, а также статусом обработки: запрещен баннер или разрешен для просмотра.

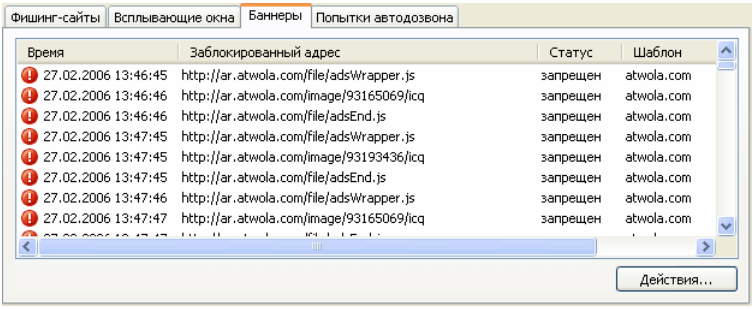


Рисунок 86. Список заблокированных баннеров

Для запрещенных баннеров вы можете разрешить их отображение. Для этого выберите в представленном списке нужный объект и воспользуйтесь кнопкой **Действия** → **Разрешить**.

17.3.11. Закладка *Попытки автодозвона*

Эта закладка (см. рис. 87) отражает все попытки скрытого дозвона на платные веб-сайты в интернете. Эти попытки, как правило, осуществляются вредоносными приложениями, установленными на вашем компьютере.

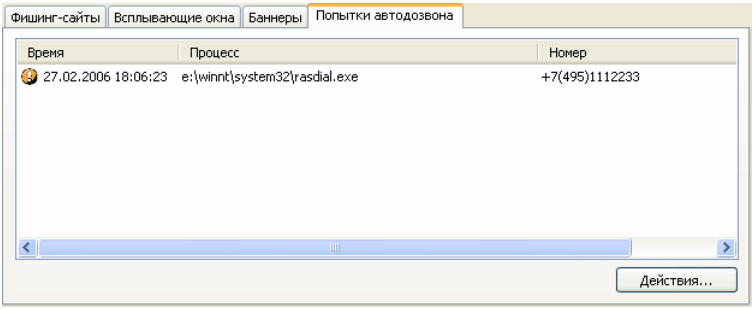


Рисунок 87. Попытки скрытого автодозвона на платные ресурсы

В этом отчете вы можете просмотреть, каким именно модулем была произведена попытка автодозвона, номер, по которому производилась попытка выхода в интернет, и статус этой попытки: заблокирована она или разрешена и по каким причинам.

17.3.12. Закладка *Сетевые атаки*

Краткий обзор сетевых атак, которым был подвергнут ваш компьютер, приводится на данной закладке (см. рис. 88). Такая информация фиксируется в том случае, если включена *Система обнаружения вторжений*, контролирующая все попытки атаковать ваш компьютер.

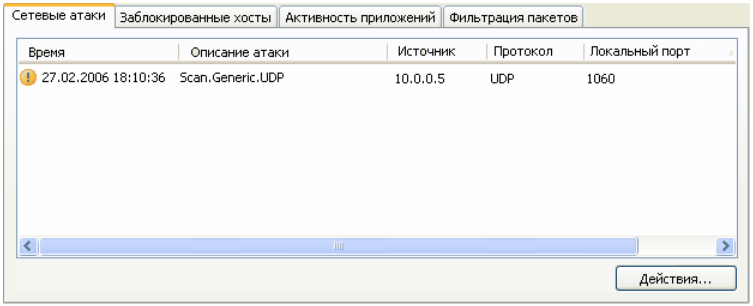


Рисунок 88. Список заблокированных сетевых атак

На закладке **Сетевые атаки** приводится следующая информация об атаке:

- Источник атаки. Это может быть IP-адрес, хост и т.п.
- Номер локального порта, на который была произведена попытка атаковать компьютер.
- Краткое описание атаки.

- Время, в которое была совершена попытка атаки.

17.3.13. Закладка *Заблокированные хосты*

Все хосты, сетевая активность по которым была заблокирована в результате обнаружения атак модулем обнаружения вторжений, приведена на данной закладке отчета (см. рис. 89).

Для каждого хоста приводится его имя и время, на которое он заблокирован. На данной закладке вы можете разблокировать хост, для этого выберите хост в списке и нажмите на кнопку **Действия → Разблокировать**.

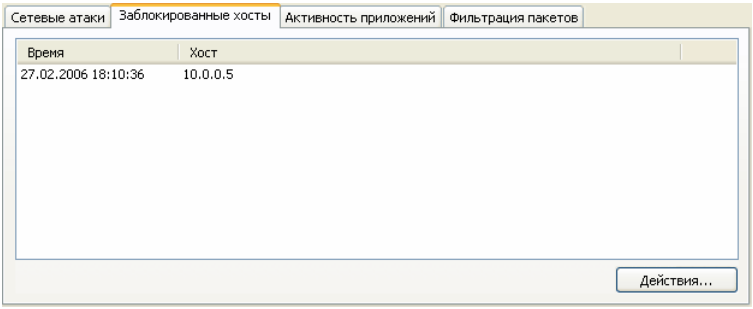


Рисунок 89. Список заблокированных хостов

17.3.14. Закладка *Активность приложений*

Все приложения, активность которых попадает под правила для приложений и была зафиксирована в текущей сессии работы Анти-Хакера модулем *Сетевой экран*, приводятся на закладке **Активность приложений** (см. рис. 90).

Активность фиксируется только в том случае, если в правиле установлен флажок **Записывать в отчет**. В правилах для приложений, включенных в поставку Антивируса Касперского, флажок по умолчанию не установлен.

Для каждого приложения указываются его основные свойства (название, PID, имя правила) и краткая характеристика его активности (протокол, направление пакета и т.д.). Также приводится информация о том, заблокирована активность приложения или нет.

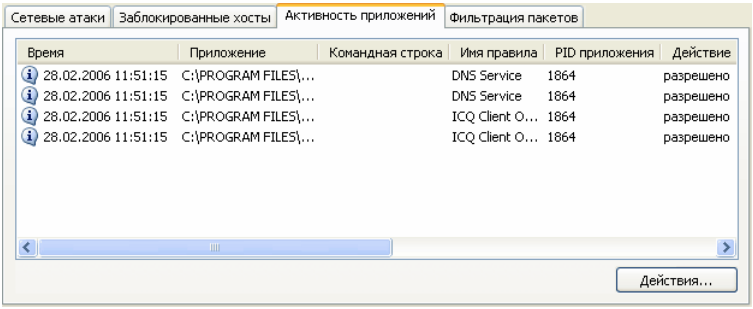


Рисунок 90. Контролируемая активность приложений

17.3.15. Закладка *Фильтрация пакетов*

На закладке **Фильтрация пакетов** (см. рис. 91) приводится информация о приеме и передаче пакетов, которые подпадают под правила фильтрации и были зафиксированы в текущей сессии работы приложения.

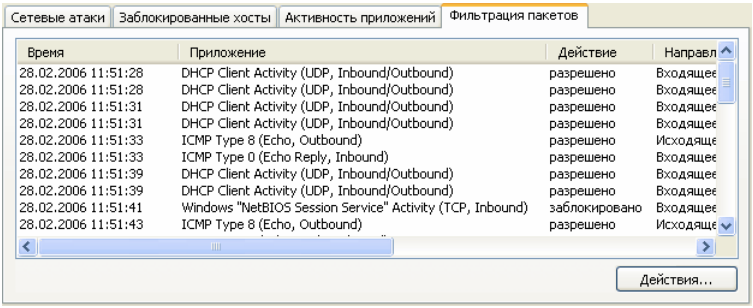


Рисунок 91. Контролируемые пакеты данных

Активность фиксируется только в том случае, если в правиле установлен флажок ☑ **Записывать в отчет**. В правилах для пакетов, включенных в поставку Антивируса Касперского, флажок не установлен.

Для каждого пакета указывается результат фильтрации (заблокирован пакет или нет), направление пакета, протокол и другие параметры сетевого соединения для приема / передачи пакета.

17.3.16. Закладка *Установленные соединения*

Все активные сетевые соединения, установленные на вашем компьютере в данный момент, приведены на закладке **Установленные соединения** (см. рис. 92). Для каждого соединения указывается имя приложения, инициировавшего его, протокол, по которому выполняется соединение, направление соединения (входящее или исходящее), параметры соединения (локальный и удаленный порты и IP-адреса). Здесь же вы можете просмотреть, как долго уже выполняется соединение и объем переданной / принятой информации. Для выбранного соединения можно создать правило или разорвать его. Для этого воспользуйтесь соответствующими пунктами контекстного меню.

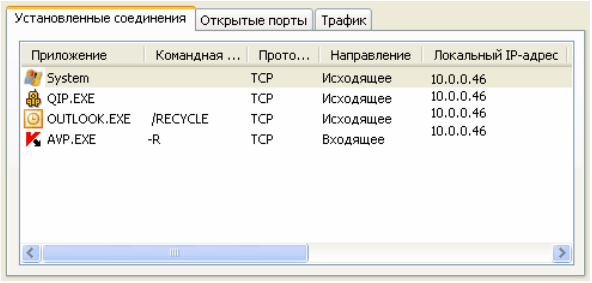


Рисунок 92. Список установленных соединений

17.3.17. Закладка *Открытые порты*

Все порты, открытые на вашем компьютере для сетевых соединений в данный момент, приведены на закладке **Открытые порты** (см. рис. 93). Для каждого порта указан его номер, протокол передачи данных, имя приложения, использующего порт, а также период времени, в течение которого порт открыт для соединения.

Такая информация может быть полезной, например, в период эпидемий и сетевых атак, когда известно, какой именно порт является уязвимым. Вы можете узнать, открыт ли такой порт на вашем компьютере и принять необходимые меры по защите вашего компьютера (например, включить Детектор атак, закрыть уязвимый порт или создать для него правило).

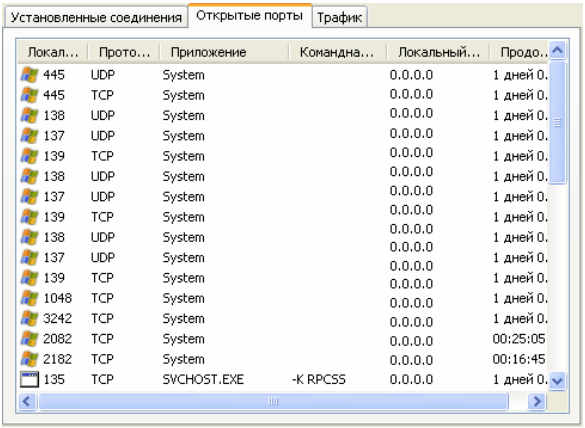


Рисунок 93. Список открытых на компьютере портов

17.3.18. Закладка *Трафик*

На этой закладке (см. рис. 94) приведена информация обо всех входящих и исходящих соединениях, которые устанавливались между вашим компьютером и другими компьютерами (в том числе веб-серверами, почтовыми серверами и т.д.). По каждому соединению приведена следующая информация: имя и IP-адрес хоста, с которым устанавливалось соединение, а также объем исходящего и входящего трафика.

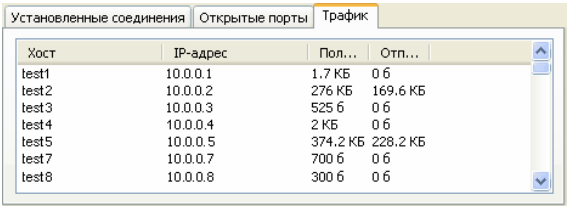


Рисунок 94. Трафик по установленным сетевым соединениям

17.4. Общая информация о приложении

Общую информацию о приложении вы можете просмотреть в разделе **Сервис** главного окна (см. рис. 95).

Вся информация разбита на три блока:

- Версия приложения, дата его последнего обновления и количество известных на настоящее время угроз приводятся в разделе **Информация о программе**.
- Краткие данные об установленной на вашем компьютере операционной системе приведены в блоке **Информация о системе**.
- Основная информация о приобретенной вами лицензии на использование Антивируса Касперского содержится в блоке **Информация о лицензии**.

Вся эта информация потребуется вам при обращении в Службу технической поддержки «Лаборатории Касперского» (см. п. 17.6 на стр. 265).

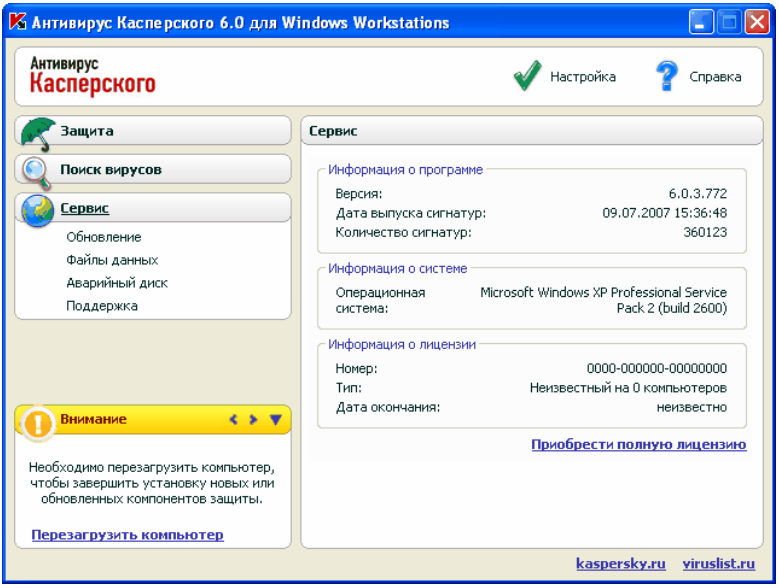


Рисунок 95. Информация о приложении, его лицензии и системе, на которую оно установлено

17.5. Управление лицензиями

Возможность использования Антивируса Касперского определяется наличием *лицензионного ключа*. Ключ предоставляется вам на основании покупки продукта и дает право использовать приложение со дня установки ключа.

Без лицензионного 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 коммерческой лицензии функциональность приложения сохраняется за исключением возможности обновления сигнатур угроз. Вы по-прежнему можете проверять ваш компьютер посредством задач поиска вирусов и использовать компоненты защиты, но только на базе сигнатур угроз, актуальных на дату окончания лицензии. Следовательно, мы не гарантируем вам стопроцентную защиту от новых вирусов, которые появятся после окончания действия лицензии приложения.

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

Чтобы продлить лицензию, вам необходимо приобрести и установить новый лицензионный ключ для приложения или указать код активации приложения. Для этого:

Свяжитесь с компанией, у которой вы купили продукт, и приобретите лицензионный ключ на использование приложения или код активации.

или:

Приобретите лицензионный ключ или код активации непосредственно в «Лаборатории Касперского», воспользовавшись гиперссылкой Приобрести лицензию в окне лицензионных ключей (см. рис. 96). Заполните соответствующую форму на открывшейся странице нашего веб-сайта. По факту оплаты на электронный адрес, указанный в форме заказа, вам будет отправлена ссылка. По этой ссылке вы сможете скачать лицензионный ключ или получить код активации приложения.

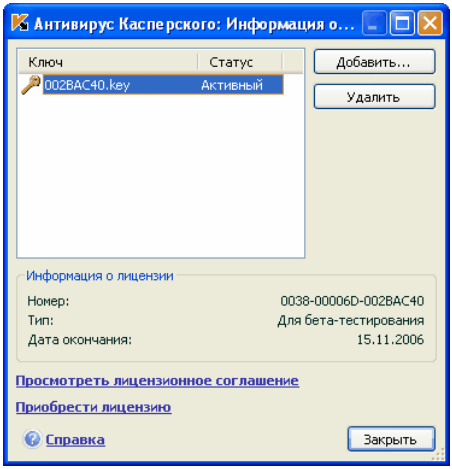


Рисунок 96. Информация о лицензии

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**.

Информация об используемом лицензионном ключе представлена в блоке **Информация о лицензии** раздела **Сервис** главного окна приложения. Для перехода в окно управления лицензиями щелкните левой клавишей мыши в любом месте блока. В открывшемся окне (см. рис. 96) вы можете просмотреть информацию о текущем ключе, добавить ключ или удалить его.

При выборе ключа в списке в блоке **Информация о лицензии** будет представлены данные о номере, типе и дате окончания лицензии. Для добавления нового лицензионного ключа воспользуйтесь кнопкой **Добавить** и активируйте приложения средствами мастера активации (см. п. 3.2.2 на стр. 41). Для удаления ключа из списка нажмите на кнопку **Удалить**.

Чтобы ознакомиться с условиями лицензионного соглашения на использование продукта воспользуйтесь ссылкой Просмотреть лицензионное соглашение. Для приобретения лицензии через веб-форму на сайте «Лаборатории Касперского» нажмите на ссылку Приобрести лицензию.

17.6. Техническая поддержка пользователей

Антивирус Касперского предоставляет вам широкие возможности решения вопросов и проблем, связанных с работой приложения. Все они размещены в **Поддержке** (см. рис. 97) раздела **Сервис**.

Рисунок 97. Информация о технической поддержке

В зависимости от проблемы, которую вы хотите решить, мы предлагаем вам воспользоваться следующими сервисами технической поддержки:

Форум пользователей. Данный ресурс является отдельным разделом веб-сайта «Лаборатории Касперского» и содержит вопросы, отзывы и пожелания пользователей приложения. Вы можете ознакомиться с основными темами форума, оставить свой отзыв о приложении или найти ответ на свой вопрос.

Чтобы перейти к этому ресурсу, воспользуйтесь ссылкой Форум пользователей.

База знаний. Данный ресурс также является отдельным разделом веб-сайта «Лаборатории Касперского» и содержит рекомендации Службы технической поддержки по работе с продуктами «Лаборатории Касперского», ответы на часто задаваемые вопросы. Попро-

буйте найти ответ на ваш вопрос или решение вашей проблемы на этом ресурсе.

Чтобы получить техническую поддержку онлайн, воспользуйтесь ссылкой База знаний.

Отзывы о работе приложения. Этот сервис предназначен для того, чтобы оставить подробный отзыв о работе приложения или описать возникшую проблему в работе приложения. Вам нужно заполнить специальную форму на веб-сайте компании, подробно описав ситуацию. Для того чтобы детально разобраться в проблеме, специалистам «Лаборатории Касперского» потребуется некоторая информация о системе. Вы можете самостоятельно описать конфигурацию системы или воспользоваться автоматическим сбором информации о вашем компьютере.

Чтобы перейти к форме отзывов, воспользуйтесь ссылкой Сообщите об ошибке или оставьте отзыв о программе.

Помощь технической поддержки. Если вам потребуется помощь в работе с Антивирусом Касперского, воспользуйтесь ссылкой, размещенной в блоке **Локальная служба технической поддержки**. В результате будет открыт веб-сайт «Лаборатории Касперского» с подробной информацией о том, как получить помощь специалистов.

17.7. Формирование списка контролируемых портов

В работе таких компонентов защиты как Почтовый Антивирус, Веб-Антивирус, Анти-Шпион и Анти-Спам 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 Антивируса Касперского по ссылке Настройка главного окна.

2. Выберите **Настройку сети** в разделе **Сервис** дерева настройки приложения.
3. В правой части окна настройки нажмите на кнопку **Настройка портов**.
4. Откорректируйте список контролируемых портов в открывшемся окне (см. рис. 98).

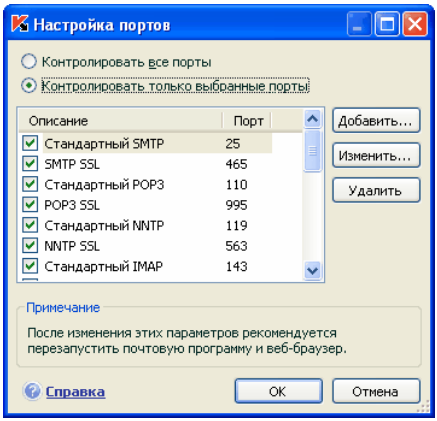


Рисунок 98. Список контролируемых портов

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 выбранные порты**.

При управлении Антивирусом Касперского 6.0, установленном на компьютере с операционной системой Microsoft Windows 98, через Kaspersky Administration Kit не рекомендуется при настройке политики выбирать вариант **Контролировать все порты**. В противном случае могут возникать проблемы доступа к сетевым ресурсам и интернету.

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.

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 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 *avp.exe*, который, в свою очередь, пытается самостоятельно установить соединение с запрашиваемой веб-страницей. Если для процесса *avp.exe* отсутствует разрешающее правило, сетевой экран заблокирует этот запрос. В результате веб-страница будет недоступна пользователю.

17.8. 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 6.0 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. 99) 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**.

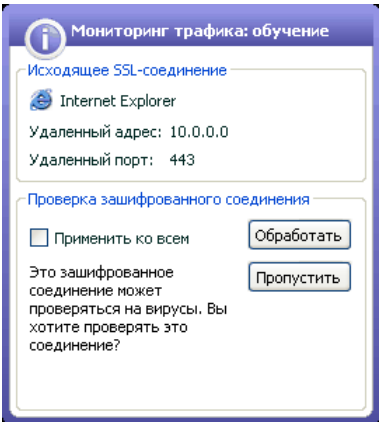


Рисунок 99. Уведомление об обнаружении SSL-соединения

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, про-

грамма MSN Messenger при установке защищенного соединения с сервером проверяет подлинность цифровой подписи Microsoft Corporation.

Настройка проверки SSL-соединения выполняется на закладке **Настройка сети** окна настройки приложения:

Проверять все защищенные соединения – проверять весь трафик, проходящий по протоколу SSL, на вирусы.

Спрашивать 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.

17.9. 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 приложения выполните следующие действия:

1. Откройте окно настройки Антивируса Касперского по ссылке Настройка главного окна.
2. Выберите **Вид** в разделе **Сервис** дерева настройки приложения (см. рис. 100).

В правой части окна настройки вы можете определить:

- 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**.

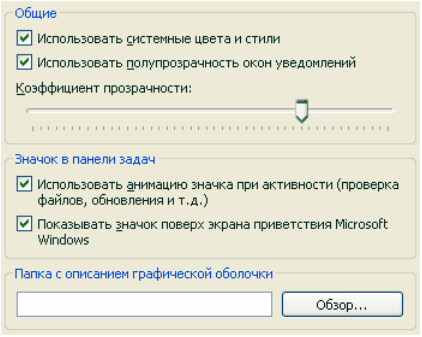


Рисунок 100. Настройка параметров интерфейса приложения

- 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 сообщение – 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.

- 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**.

  Данная возможность недоступна в приложении, установленном на компьютере под управлением операционной системы Microsoft Windows 98/NT 4.0/ME.

- Использование собственных графических элементов и цветовой палитры в интерфейсе приложения.

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 **Каталог с описанием графической оболочки**. Для выбора каталога воспользуйтесь кнопкой **Обзор**.

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.

Обратите внимание, что изменение параметров интерфейса Антивируса Касперского не сохраняется при восстановлении параметров работы по умолчанию или удалении приложения.

17.10. Диск аварийного восстановления

В Антивирусе 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 Антивируса Касперского;
- файлы, содержащие сигнатуры угроз.

Чтобы создать диск аварийного восстановления:

1. Откройте главное окно приложения и выберите **Аварийный диск** в разделе **Сервис**.
2. Нажмите на кнопку **Запуск мастера** 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, установленом 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.

17.10.1. 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:

- Каталогу установки программы PE Builder.
- Каталогу хранения файлов диска аварийного восстановления перед записью на CD-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 старые сигнатуры угроз. Чтобы обеспечить оптимальный анализ компьютера на вирусы и восстановление системы, рекомендуется обновить сигнатуры угроз и создать новую версию диска аварийного восстановления.

- Установочному диску Microsoft Windows XP Service Pack 2.

Для создания диска аварийного восстановления, позволяющего загружать операционную систему на удаленном компьютере с последующей проверкой и обработкой вредоносных объектов Антивирусом Касперского, установите флажок **Разрешить удаленное управление проверяемым компьютером**.

Обратите внимание, что для использования данной возможности удаленный компьютер должен поддерживать технологию Intel® vPRO™ или Intel® Active Management Technology (iAMT). Данные технологии позволяют администраторам удаленно обращаться ко всем подключенным к сети компьютерам, в том числе к тем, которые выключены и на которых нарушена работоспособность операционной системы или жесткого диска.

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-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-диск: в данный момент или позже.

Если вы выбрали немедленную запись диска, укажите, нужно ли очистить содержимое CD-носителя перед записью. Для этого установите соответствующий флажок. Данная возможность доступна только в случае, если CD-носитель поддерживает многократную перезапись данных (CD-RW).

При нажатии на кнопку **Далее** начнется процесс записи CD-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.

17.10.2. Использование диска аварийного восстановления

Обратите внимание, что в режиме аварийного восстановления Антивирус Касперского работает, только если запущено главное окно. При закрытии главного окна приложение будет выгружено.

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 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 сигнатуры угроз из локальной сети. Если обновление не требуется, отмените включение сетевой поддержки.

3. Для запуска Антивируса Касперского выполните команду **GO** → **Programs** → **Kaspersky Anti-Virus 6.0 для Windows Workstations** → **Start**.

   В результате будет запущено главное окно Антивируса Касперского. В режиме аварийного восстановления доступны только задачи поиска вирусов и обновление сигнатур угроз 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 сигнатуры угроз, актуальные на дату создания диска аварийного восстановления. Поэтому перед началом проверки рекомендуется обновить базы сигнатур угроз.

Также обращаем внимание, что обновленные базы сигнатур угроз 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.

17.11. Использование дополнительных сервисов

Антивирус Касперского предлагает вам воспользоваться следующими дополнительными сервисами:

- Уведомление пользователя по электронной почте о возникновении некоторых событий в работе приложения.
- Самозащита Антивируса Касперского от выключения, удаления или изменения модулей, а также защита доступа к приложению паролем.
- Решение проблем совместимости Антивируса Касперского 6.0 при работе с другими приложениями.

Чтобы перейти к настройке использования перечисленных сервисов,

1. Откройте окно настройки приложения по ссылке Настройка главного окна.
2. Выберите пункт **Сервис** в дереве настройки.

В правой части вы можете определять, использовать дополнительные сервисы в работе приложения или нет.

17.11.1. 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 **Взаимодействие с пользователем** (см. рис. 101).

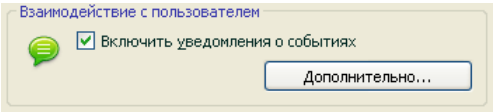


Рисунок 101. Включение режима уведомлений

2. Определить типы событий Антивируса Касперского, о возникновении которых вы хотите быть уведомлены, и способ уведомлений (см. п. 17.11.1.1 на стр. 278).

3. Настроить параметры отправки уведомлений по электронной почте, если предполагается именно такой способ уведомлений (см. п. 17.11.1.2 на стр. 280).

17.11.1.1. 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, *сигнатуры угроз повреждены* или *истек срок действия лицензии*.

Отказ функциональности – события, приводящие к неработоспособности приложения. Например, отсутствие лицензии и сигнатур угроз.

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. Нажмите на ссылку Настройка в главном окне приложения.
2. В окне настройки приложения выберите раздел **Сервис**, установите флажок ☑ **Включить уведомление о событиях** и перейдите к детальной настройке по кнопке **Дополнительно**.

В открывшемся окне **Настройка уведомлений** (см. рис. 102) 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.

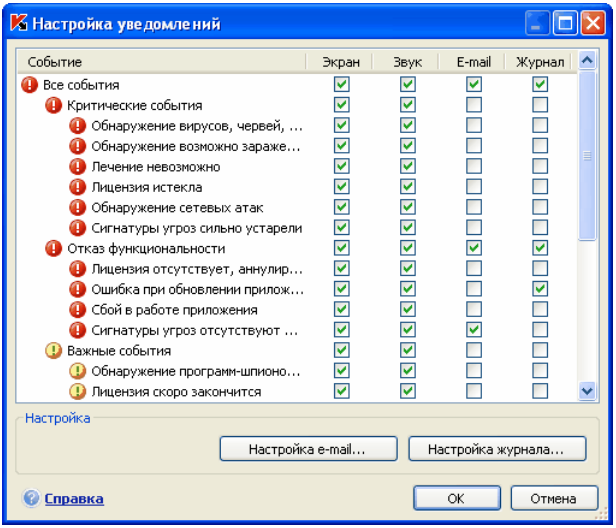


Рисунок 102. События в работе приложения и способы уведомлений о них

- 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. 17.11.1.2 на стр. 280).

- Запись информации в журнал событий.

  Чтобы фиксировать информацию о наступлении какого-либо события в журнале, установите напротив него флажок ☑ графе **Журнал** и настройте параметры журнала событий (см. п. 17.11.1.3 на стр. 281).

17.11.1.2. Настройка отправки уведомлений по электронной почте

После того как вы выбрали события (см. п. 17.11.1.1 на стр. 278), уведомления о возникновении которых вы хотите получать по электронной почте, необходимо настроить отправку уведомлений. Для этого:

1. Откройте окно настройки приложения по ссылке Настройка главного окна.
2. Выберите пункт **Сервис** в дереве настройки.
3. Нажмите на кнопку **Дополнительно** в блоке **Взаимодействие с пользователем** правой части окна.
4. На закладке **Настройка уведомлений** (см. рис. 102) установите в графе **E-mail** флажок ☑ для событий, при наступлении которых требуется отправлять уведомление по электронной почте.
5. В окне, открывающемся 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 отправляло 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.

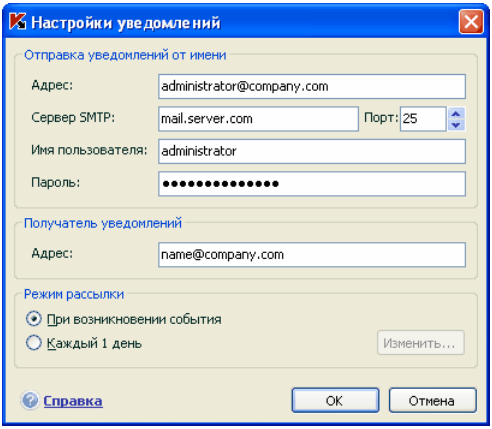


Рисунок 103. Настройка параметров уведомления по электронной почте

17.11.1.3. Настройка параметров журнала событий

Чтобы настроить параметры журнала событий:

1. Откройте окно настройки приложения по ссылке Настройка главного окна.
2. Выберите пункт **Сервис** в дереве настройки.
3. Нажмите на кнопку **Дополнительно** в блоке **Взаимодействие с пользователем** правой части окна.

В окне **Настройка уведомлений** выберите для какого-либо события возможность записи информации в журнал и нажмите на кнопку **Настройка 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**).

На компьютере под управлением операционной системы Microsoft Windows 98/ME ведение журналов событий недоступно, а под управлением Microsoft Windows NT 4.0 недоступна запись в журнал **Kaspersky Event Log**.

Эти ограничения обусловлены особенностями данных операционных систем.

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

17.11.2. Самозащита приложения и ограничение доступа к нему

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

В Антивирусе Касперского, установленном на компьютере под управлением операционной системы Microsoft Windows 98/ME, недоступно использование сервиса самозащиты приложения.

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 по ссылке Настройка главного окна.
2. Выберите пункт **Сервис** в дереве настройки.
3. В блоке **Самозащита** (см. рис. 104) 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).

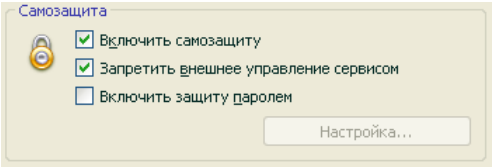


Рисунок 104. Настройка защиты приложения

Чтобы защитить доступ к приложению с помощью пароля, установите флажок **Включить защиту паролем** и в окне, открывающемся по кнопке **Настройка**, укажите пароль и область, на которую будет распространяться ограничение доступа (см. рис. 105). Вы можете заблокировать любые операции с приложением, за исключением работы с уведомлениями 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.

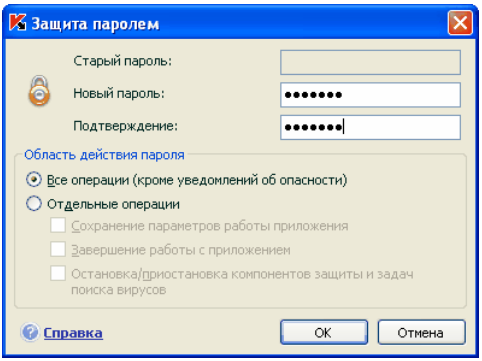


Рисунок 105. Настройка защиты приложения паролем

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.

17.11.3. 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 Oxygen Phone Manager II, а также некоторые виды игр, имеющие защиту от взлома.

Для решения данной проблемы установите флажок **Совместимость с самозащитой приложений** в разделе **Сервис** окна настройки приложения. Для вступления изменений данного параметра в силу требуется перезагрузка операционной системы.

Если приложение установлено на компьютер под управлением Microsoft Windows Vista и Microsoft Windows Vista x64, возможность решения проблем совместимости с самозащитой других приложений не поддерживается.

Однако обратите внимание, что при включенном флажке часть функциональности Антивируса Касперского, а именно проверка VBA-макросов, Анти-Дозвон, работать не будет. При включении любого из этих компонентов режим совместимости в самозащитой приложений будет автоматически отключен. После включения данные компоненты начнут работать только после перезагрузки операционной системы.

17.12. Экспорт / импорт параметров работы Антивируса Касперского

Антивирус Касперского предоставляет вам возможность экспорта и импорта своих параметров.

Это полезно, например, в том случае, когда приложение установлено 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 главное окно Антивируса Касперского.
2. Выберите раздел **Сервис** и нажмите на ссылку Настройка.
3. Нажмите на кнопку **Сохранить** в блоке **Управление конфигурацией**.
4. Введите название конфигурационного файла и укажите место его сохранения.

Для импорта параметров работы из конфигурационного файла

1. Откройте главное окно Антивируса Касперского.
2. Выберите раздел **Сервис** и нажмите на ссылку Настройка.
3. Нажмите на кнопку **Загрузить** и выберите файл, из которого вы хотите импортировать параметры Антивируса Касперского.

17.13. 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. Выберите раздел **Сервис** и по ссылке Настройка перейдите в окно настройки приложения.
2. Нажмите на кнопку **Восстановить** в разделе **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 или накоплены приложением в результате обучения (Анти-Хакер и Анти-Спам). Если для какого-либо из компонентов в процессе работы были сформированы уникальные параметры, они также будут представлены в списке.

Такими уникальными параметрами являются «белые» и «черные» списки фраз и адресов, используемых Анти-Спамом, списки доверенных интернет-адресов и телефонных номеров интернет-провайдеров, используемых Веб-Антивирусом и Анти-Шпионом, сформированные правила исключений защиты для компонентов приложения, правила фильтрации пакетов и приложений Анти-Хакера, 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 настроек 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. 40). 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.

ГЛАВА 18. 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 сигнатур угроз и модулей приложения;
- вызов справки по синтаксису командной строки;
- вызов справки по синтаксису команды.

Синтаксис командной строки:

```
avp.com <команда> [параметры]
```

Обращение к приложению через командную строку должно осуществляться из каталога установки продукта либо с указанием полного пути к avp.com.

В качестве **<команд>** используются:

ADDKEY	активация приложения с помощью файла ключа (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
ACTIVATE	активация приложения через интернет с помощью кода активации
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 Антивируса Касперского (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
EXPORT	экспорт параметров защиты Антивируса Касперского

Каждой команде соответствует собственный набор параметров, специфичный для конкретного компонента Антивируса Касперского.

18.1. Активация приложения

Активацию приложения возможно произвести двумя способами:

- через интернет с помощью кода активации (команда ACTIVATE);
- с помощью файла лицензионного ключа (команда ADDKEY).

Синтаксис команды:

```
ACTIVATE <код_активации>
ADDKEY <имя_файла> /password=<ваш_пароль>
```

Описание параметров:

<имя_файла>	имя файла ключа к приложению с расширением **.key*.
<код_активации>	код активации приложения, предоставленный при покупке.
<ваш_пароль>	пароль к Антивирусу Касперского, заданный в интерфейсе приложения.
Обратите внимание, что без ввода пароля данная команда выполняться не будет.	

Пример:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<ваш_пароль>
```

18.2. 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 выполняется с помощью следующего набора команд: **START** – запуск компонента постоянной защиты или задачи. **STOP** – остановка работы компонента постоянной защиты или задачи. **PAUSE** – приостановка работы компонента постоянной защиты или задачи. **RESUME** – возобновление работы компонента постоянной защиты или задачи. **STATUS** – вывод на экран текущего статуса компонента постоянной защиты или задачи. **STATISTICS** – вывод на экран статистики по работе компонента постоянной защиты или задачи. Обратите внимание, что без ввода пароля команды PAUSE и STOP выполняться не будут.
<профайл|имя_задачи>	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). В качестве значений для параметра **<имя_задачи>** может быть указано имя любой сформированной пользователем задачи проверки по требованию либо обновления.
<ваш_пароль>	пароль к Антивиурсу Касперского, заданный в интерфейсе приложения.
/R[A]:<файл_отчета>	**R:<файл_отчета>** – фиксировать в отчете только важные события. **/RA:<файл_отчета>** – записывать в отчет все

	события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

В качестве параметра **<профайл>** указывается одно из следующих значений:

RTP	все компоненты защиты Команда `avp.com START RTP` запускает все компоненты постоянной защиты, если защита была полностью отключена (см. п. 6.1.2 на стр. 75) либо приостановлена на время (см. п. 6.1.1 на стр. 74). Также данная команда запускает любой из компонентов постоянной защиты, работа которого приостановлена кнопкой ❚❚ графического интерфейса либо командой `PAUSE` командной строки. В случае если компонент был отключен кнопкой ■ графического интерфейса либо командой `STOP` командной строки, он не будет запущен командой `avp.com START RTP`. Для этого необходимо выполнить команду `avp.com START <профайл>`, где в качестве <профайл> используется значение для конкретного компонента защиты, например, `avp.com START FM`.
FM	Файловый Антивирус
EM	Почтовый Антивирус
WM	Веб-Антивирус Значения для подкомпонентов Веб-Антивиурса: **httpscan** – проверка http-трафика; **sc** – проверка скриптов.
BM	Проактивная защита Значения для подкомпонентов Проактивной защиты:

	og – проверка макросов Microsoft Office; **pdm** – анализ активности приложений.
ASPY	Анти-Шпион Значения для подкомпонентов Анти-Шпиона: **AdBlocker** – анти-реклама; **antidial** – анти-дозвон; **antiphishing** – анти-фишинг; **popupchk** – анти-баннер.
AH	Анти-Хакер Значения для подкомпонентов Анти-Хакера: **fw** – сетевой экран; **ids** – система обнаружения вторжений.
AS	Анти-Спам
UPDATER	Обновление
RetranslationCfg	Копирование обновлений в локальный источник
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
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>
```

18.3. 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. 18.1 на стр. 289). 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>	Список путей к файлам и/или каталогам для проверки. Допускается ввод абсолютного или относительного пути. Разделительный символ для элементов списка – пробел. Замечания: • 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>	путь к файлу со списком объектов и каталогов, включаемых в проверку. Файл должен иметь текстовый формат; каждый объект проверки необходимо указывать с новой строки. Допускается ввод абсолютного или относительного пути к файлу. Путь указывается в кавычках, если в нем содержится символ «пробел».
<действие> – параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению **/i8**.	
/i0	не совершать над объектом никаких действий, только фиксировать информацию о нем в отчете.

/i1	лечить зараженные объекты, если лечение невозможно – пропустить.
/i2	лечить зараженные объекты, если лечение невозможно – удалять; не удалять зараженные объекты из контейнеров (составных объектов); удалять контейнеры с исполняемым заголовком (sfx-архивы) (данное действие используется по умолчанию).
/i3	лечить зараженные объекты, если лечение невозможно – удалять; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
/i4	удалять зараженные объекты; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
/i8	запрашивать действие у пользователя при обнаружении зараженного объекта.
/i9	запрашивать действие у пользователя по окончании проверки.
<типы файлов> - параметр определяет типы файлов, которые будут подвергаться антивирусной проверке. По умолчанию, если параметр не задан, проверяются только заражаемые файлы по содержимому.	
/fe	проверять только заражаемые файлы по расширению.
/fi	проверять только заражаемые файлы по содержимому.
/fa	проверять все файлы.
<исключения> - параметр определяет объекты, исключаемые из проверки. Параметр может включать несколько значений из представленного списка, разделенных пробелом.	
-e:a	не проверять архивы.

-e:b	не проверять почтовые базы.
-e:m	не проверять почтовые сообщения в формате plain text.
-e:<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>**.

<конфигурационный файл> - определяет путь к конфигурационному файлу, содержащему параметры работы приложения при проверке.

Конфигурационный файл представляет собой файл текстового формата, содержащий набор параметров командной строки для антивирусной проверки.

Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе Антивируса Касперского.

/C:<имя_файла>	использовать значения параметров, заданные в конфигурационном файле **<имя_файла>**.

<параметры отчета> - параметр определяет формат отчета о результатах проверки.

Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

/R:<файл_отчета>	записывать в указанный файл отчета только важные события.
/RA:<файл_отчета>	записывать в указанный файл отчета все события.

<дополнительные параметры> – параметр, определяющий использование технологий антивирусной проверки.

/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 /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

Пример конфигурационного файла:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

18.4. Обновление приложения

Команда для обновления модулей приложения и сигнатур угроз Антивируса Касперского имеет следующий синтаксис:

```
avp.com UPDATE [<источник_обновлений>]
[/R[A]:<файл_отчета>] [/C:<имя_файла>] [/APP=<on|off>]
```

Описание параметров:

<источник_обновлений>	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.
/R[A]:<файл_отчета>	**/R:<файл_отчета>** - фиксировать в отчете только важные события. **/RA:<файл_отчета>** - записывать в отчет все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.
/C:<имя_файла>	путь к конфигурационному файлу, содержащему параметры работы приложения при обновлении. Конфигурационный файл представляет собой файл текстового формата, содержащий набор параметров командной строки для обновления приложения. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения параметров, установленные в интерфейсе Антивируса Касперского.
/APP=<on|off>	включить/ отключить обновление модулей приложения.

Примеры:

Обновить сигнатуры угроз, 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
```

18.5. Откат последнего обновления приложения

Синтаксис команды:

```
ROLLBACK [/R[A]:<файл_отчета>][/password=<ваш_пароль>]
```

/R[A]:<файл_отчета>	**/R:<файл_отчета>** - фиксировать в отчете только важные события. **/RA:<файл_отчета>** - записывать в отчет все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.
<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>
```

18.6. Экспорт параметров защиты

Синтаксис команды:

```
avp.com EXPORT <профайл> <имя_файла>
```

Описание параметров:

<профайл>	компонент или задача, для которых выполняется экспорт параметров. В качестве значения параметра **<профайл>** может быть использовано любое значение, указанное в п. 18.2 на стр. 289.
<имя_файла>	путь к файлу, в который экспортируются параметры Антивируса Касперского. Может быть указан абсолютный или относительный путь. Конфигурационный файл сохраняется в бинарном формате (*dat*), 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 *txt*. Обратите внимание, что импорт параметров защиты из текстового файла не поддерживается, данный файл может использоваться только для просмотра основных параметров работы приложения.

Пример:

```
avp.com EXPORT c:\settings.dat
```

18.7. 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. При установке приложения в скрытом режиме через командную строку или Редактор объектов групповой политики имя конфигурационного файла должно быть *install.cfg*, иначе он не будет

	распознаваться приложением.
<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>
```

18.8. Запуск приложения

Синтаксис команды:

```
avp.com
```

18.9. 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.	

18.10. 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>]
```

[on|off]	Включить/ отключить создание файла трасси-

	ровки.
[file]	Получить трассировку в виде файла.
<уровень_трассировки>	Для данного параметра допустимо указывать числовое значение в диапазоне от 0 (минимальный уровень, только критические сообщения) до 700 (максимальный уровень, все сообщения). При обращении в Службу технической поддержки специалист должен указать необходимый уровень трассировки. Если он не был указан, то рекомендуется устанавливать уровень 500.
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
```

18.11. 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>
```

18.12. 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 антивирусной проверки	
101	Все опасные объекты обработаны
102	Обнаружены опасные объекты

ГЛАВА 19. ИЗМЕНЕНИЕ, ВОССТАНОВЛЕНИЕ ИЛИ УДАЛЕНИЕ ПРИЛОЖЕНИЯ

Удалить приложение вы можете следующими способами:

- с помощью мастера установки приложения (см. п. 19.1 на стр. 304);
- из командной строки (см. п. 19.2 на стр. 307);
- через Kaspersky Administration Kit (см. «Руководство по внедрению Kaspersky Administration Kit»);
- через доменные групповые политики Microsoft Windows Server 2000/2003 (см. п. 3.4.3 на стр. 53).

19.1. 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. 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 в данном источнике и у вас есть к нему доступ.

2. Выберите **Пуск → Программы → Kaspersky Anti-Virus 6.0 для Windows Workstations → 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. Стартовое окно программы установки

Если вы провели все описанные выше действия, необходимые для восстановления или изменения состава приложения, на экране будет открыто приветственное окно программы установки Антивируса Касперского. Для продолжения нажмите на кнопку **Далее**.

Шаг 2. Выбор операции

На данном этапе вам нужно определить, какую именно операцию вы хотите выполнить над 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 7 на стр. 38), 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, необходимый для работы приложения.
- *Сигнатуры угроз* – полный набор сигнатур опасных программ, вирусов и других угроз, актуальный на дату последнего обновления.

- *База Анти-Спама* – база данных, на основе которой распознается нежелательная электронная корреспонденция. Эта база содержит подробную информацию о том, какая почта является для вас спамом, а какая – полезной почтой.
- *Объекты резервного хранилища* – резервные копии удаленных или вылеченных объектов. Такие объекты рекомендуется сохранить для возможности последующего восстановления.
- *Объекты карантина* – объекты, возможно зараженные вирусами или их модификациями. Такие объекты содержат код, который похож на код известного вируса, но однозначно судить об их вредоносности нельзя. Рекомендуется их сохранить, поскольку они могут оказаться незараженными или их излечение будет возможно после обновления сигнатур угроз.
- *Параметры защиты* – значения параметров работы всех компонентов 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 3. Завершение операции восстановления, изменения или удаления приложения

Процесс восстановления, изменения или удаления будет отображаться на экране, после чего вы будете уведомлены о его завершении.

Удаление, как правило, требует последующей перезагрузки компьютера, поскольку это необходимо для учета изменений в системе. Запрос на перезагрузку компьютера будет выведен на экран. Нажмите на кнопку **Да**, чтобы

выполнить перезагрузку немедленно. Для того чтобы перезагрузить компьютер позже вручную, нажмите на кнопку **Нет**.

19.2. Удаление приложения из командной строки

Для того чтобы удалить Антивирус Касперского 6.0 для Windows Workstations из командной строки, наберите:

```
msiexec /x <имя_пакета>
```

Будет запущен мастер установки, с помощью которого вы сможете провести процедуру удаления приложения (см. п. Глава 19 на стр. 304).

Для того чтобы удалить приложение в неинтерактивном режиме без перезагрузки компьютера (перезагрузку следует произвести вручную после удаления), наберите:

```
msiexec /x <имя_пакета> /qn
```

Для того чтобы удалить приложение в неинтерактивном режиме с последующей перезагрузкой компьютера, наберите:

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

Если при установке приложения был задан пароль на запрет удаления приложения, при удалении продукта необходимо указать данный пароль, иначе процедура удаления не будет осуществлена.

Для того чтобы удалить приложение с вводом пароля, подтверждающего право на удаление приложения, наберите:

`msiexec /x <имя_пакета> KLUNINSTPASSWD=******` – для удаления приложения в интерактивном режиме;

`msiexec /x <имя_пакета> KLUNINSTPASSWD=****** /qn` – для удаления приложения в неинтерактивном режиме.

ГЛАВА 20. УПРАВЛЕНИЕ ПРИЛОЖЕНИЕМ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit – это система централизованного решения основных административных задач по управлению системой безопасности компьютерной сети предприятия, построенной на основе приложений, входящих в состав продуктов Антивирус Касперского Business Optimal и Kaspersky Corporate Suite.

Антивирус Касперского 6.0 для Windows Workstations один из продуктов «Лаборатории Касперского», управление которым возможно через собственный интерфейс приложения, командную строку (эти способы описаны выше в данной документации) либо посредством приложения Kaspersky Administration Kit (если компьютер включен в состав системы удаленного централизованного управления).

Для управления Антивирусом Касперского 6.0 для Windows Workstations через Kaspersky Administration Kit выполните следующие действия:

- разверните в сети *Сервер администрирования*; установите *Консоль администрирования* на рабочее место администратора (подробнее смотрите Руководство по внедрению «Kaspersky Administration Kit 6.0»);
- на компьютерах сети разверните Антивирус Касперского 6.0 для Windows Workstations и *Агент администрирования* (входящий в состав Kaspersky Administration Kit). Подробнее об удаленной установке пакета Антивируса Касперского на компьютеры сети смотрите Руководство по внедрению «Kaspersky Administration Kit 6.0».

При использовании Антивируса Касперского через Kaspersky Administration Kit обратите внимание на следующие особенности!

Если на компьютерах сети развернут Антивирус Касперского версии 5.0, при обновлении до версии 6.0 через Kaspersky Administration Kit выполните следующие требования:

- предварительно остановите предыдущую версию приложения (это можно сделать удаленно через Kaspersky Administration Kit);
- перед началом установки закройте все работающие приложения;
- по завершении установки выполните перезагрузку операционной системы на удаленном компьютере.

Перед обновлением версии плагина управления Антивирусом Касперского через Kaspersky Administration Kit завершите работу Консоли администрирования.

Доступ к управлению приложением через Kaspersky Administration Kit обеспечивает Консоль администрирования (см. рис. 106). Она представляет собой стандартный **интерфейс, интегрированный в MMC**, и позволяет администратору выполнять следующие функции:

- удаленно устанавливать Антивирус Касперского 6.0 для Windows Workstations и *Агент администрирования* на компьютеры сети;
- удаленно настраивать Антивирус Касперского 6.0 на компьютерах сети;
- обновлять сигнатуры угроз и модули Антивируса Касперского;
- осуществлять управление лицензиями для Антивируса Касперского на компьютерах сети;
- просматривать информацию о работе приложения на клиентских компьютерах.

При работе через Kaspersky Administration Kit управление осуществляется через определение администратором параметров политик, параметров задач и параметров приложения.

Параметры приложения – набор параметров работы приложения, включающий общие параметры защиты, параметры резервного хранилища, карантина, параметры формирования отчетов и др.

Задача – именованное действие, выполняемое приложением. В соответствии с функциями задачи Антивируса Касперского 6.0 разделяют по типам (задача поиска вирусов, задача обновления приложения, отката обновлений, задача установки лицензионного ключа). Каждой конкретной задаче

соответствует набор параметров работы приложения при ее выполнении – *параметры задачи*.

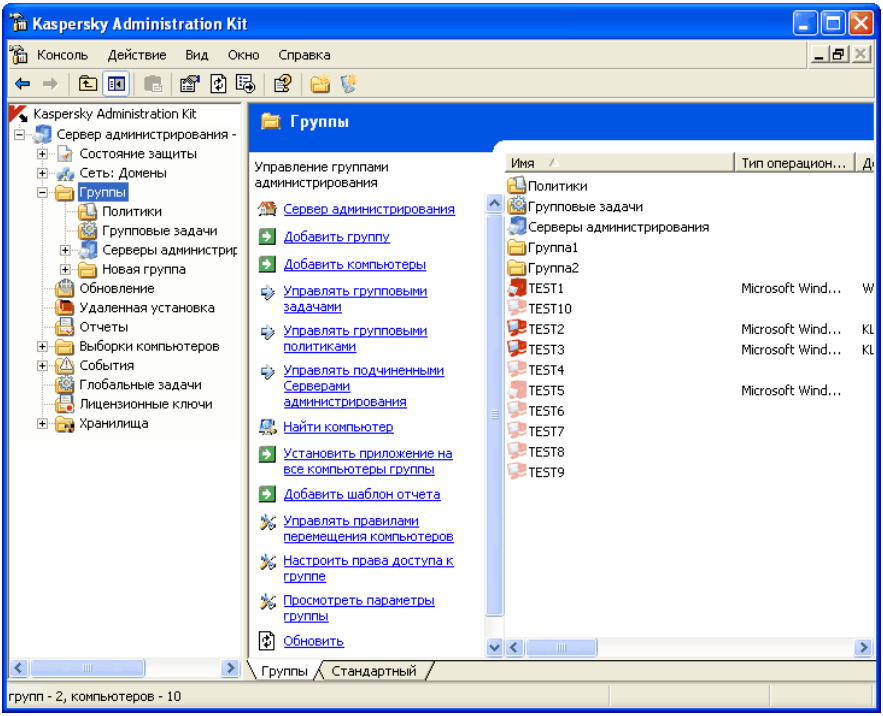


Рисунок 106. Консоль администрирования Kaspersky Administration Kit[3]

Особенностью централизованного управления является организация удаленных компьютеров сети в группы и управление ими через создание и определение групповых политик.

Политика – это набор параметров работы приложения на компьютерах группы логической сети, а также набор ограничений на переопределение данных параметров при настройке приложения или настройке задачи на отдельном клиентском компьютере.

Политика включает в себя параметры полной настройки всей функциональности приложения. Таким образом, в политику входят параметры приложения, параметры всех типов задач, за исключением специфичных для конкретного типа задачи.

[3] Вид главного окна Kaspersky Administration Kit может различаться в зависимости от используемой на компьютере операционной системы.

20.1. Управление приложением

Kaspersky Administration Kit предоставляет возможность удаленного управления запуском и остановкой Антивируса Касперского 6.0 на отдельном клиентском компьютере, а также настройки общих параметров работы приложения, таких как включение/ отключение защиты компьютера, настройка параметров резервного и карантинного хранилищей, параметров формирования отчетов.

Для управления параметрами приложения:

1. В папке **Группы** (см. рис. 106) выберите папку с названием группы, в состав которой входит клиентский компьютер.
2. В панели результатов выберите компьютер, для которого вам необходимо изменить параметры приложения, и воспользуйтесь командой **Приложения** контекстного меню или аналогичным пунктом в меню **Действие**.
3. В окне свойств клиентского компьютера на закладке **Приложения** (см. рис. 107) представлен полный список всех приложений «Лаборатории Касперского», установленных на клиентском компьютере. Выберите приложение **Антивирус Касперского 6.0 для Windows Workstations**.

Под списком приложений расположены кнопки управления, с помощью которых вы можете:

- просмотреть список событий в работе приложения, произошедших на клиентском компьютере и зарегистрированных на Сервере администрирования;
- просмотреть текущую статистическую информацию о работе приложения;
- произвести настройку параметров приложения (см. п. 20.1.2 на стр. 313).

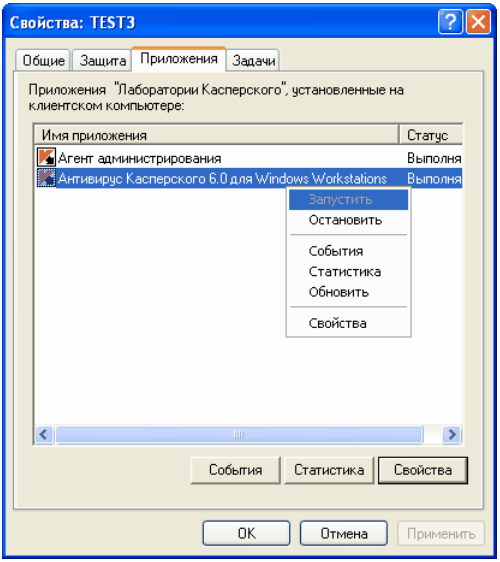


Рисунок 107. Список приложений «Лаборатории Касперского»

20.1.1. Запуск / остановка приложения

Управление запуском/ остановкой Антивируса Касперского 6.0 на удаленном клиентском компьютере осуществляется с помощью команд контекстного меню в окне свойств компьютера (см. рис. 107).

Аналогичные действия можно выполнить с помощью кнопок **Запустить** / **Остановить** из окна настройки параметров приложения на закладке **Общие** (см. рис. 108).

В верхней части окна приведено название установленного приложения, информация о версии, дата установки, его статус (запущено или остановлено приложение на локальном компьютере), а также информация о состоянии баз сигнатур угроз.

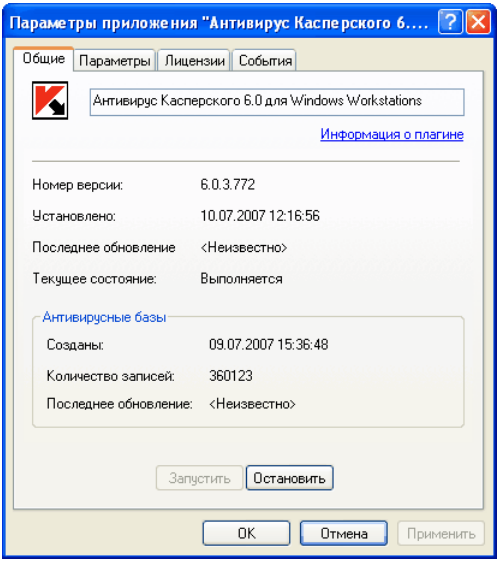


Рисунок 108. Настройка параметров Антивируса Касперского. Закладка **Общие**

20.1.2. Настройка параметров приложения

Для того чтобы просмотреть или изменить параметры работы приложения:

1. Откройте окно свойств клиентского компьютера на закладке **Приложения** (см. рис. 107).
2. Выберите приложение **Антивирус Касперского 6.0 для Windows Workstations** и воспользуйтесь кнопкой **Свойства**. В результате будет открыто окно настройки параметров приложения (см. рис. 109).

Все закладки (кроме закладки **Параметры**) являются стандартными для приложения Kaspersky Administration Kit 6.0, их подробное описание смотрите в одноименном Руководстве администратора.

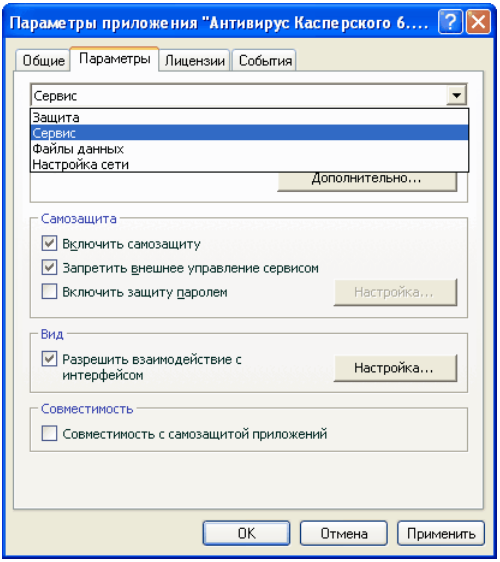


Рисунок 109. Настройка параметров Антивируса Касперского. Закладка **Параметры**

Если для приложения создана политика (см. п. 20.3 на стр. 323), в которой запрещено переопределение некоторых параметров, то их изменение при настройке параметров приложения будет недоступно.

На закладке **Параметры** вы можете настраивать общие и сервисные параметры защиты Антивируса Касперского, параметры резервного хранилища, карантина, сервиса формирования отчетов, а также параметры сети. Для этого из раскрывающегося списка в верхней части окна выберите нужное значение и произведите настройку:

Защита
В этом окне вы можете: • включать/ отключать защиту компьютера (см. п. 6.1 на стр. 73); • настраивать автоматический запуск приложения при включении компьютера (см. п. 6.1.5 на стр. 77); • формировать список исключений из проверки (см. п. 6.3 на стр. 79); • выбирать категории вредоносного программного обеспечения, которые будут контролироваться приложением (см. п. 6.2 на стр. 78);

- настраивать параметры производительности работы Антивируса Касперского (см. п. 6.6 на стр. 91).

Сервис

Настройка сервисных параметров включает в себя:

- настройку сервиса получения уведомлений о событиях, возникающих в работе приложения (см. п. 17.11.1 на стр. 277);
- управление сервисом самозащиты Антивируса Касперского и ограничения доступа к нему с помощью пароля (см. п. 17.11.2 на стр. 282);
- настройку внешнего вида приложения на удаленном компьютере, является специфической настройкой Антивируса Касперского при управлении через Kaspersky Administration Kit (см. п. 20.1.3 на стр. 316);
- настройку парметров совместимости Антивируса Касперского с другими приложениями (см. п. 17.11.3 на стр. 284).

Файлы данных

В данном окне вам предлагается настроить параметры формирования отчетной статистики по работе приложения (см. п. 17.3.1 на стр. 249), а также указать время хранения файлов в резервном хранилище (см. п. 17.1.2 на стр. 243) и на карантине (см. п. 17.2.2 на стр. 246).

Настройка сети

В данном окне вы можете отредактировать список портов, используемых Антивирусом Касперского для проверки (см. п. 17.7 на стр. 266), а также включить/ отключить проверку зашифрованных соединений по протоколу SSL (см. п. 17.8 на стр. 268).

20.1.3. Настройка специфических параметров

При управлении Антивирусом Касперского через Kaspersky Administration Kit вы можете включать/ отключать режим взаимодействия приложения с пользователем, а также редактировать информацию о технической поддержке. Для этого:

1. Откройте окно свойств клиентского компьютера на закладке **Приложения** (см. рис. 107). Выберите приложение **Антивирус Касперского 6.0 для Windows Workstations** и воспользуйтесь кнопкой **Свойства**. В результате будет открыто окно настройки параметров приложения.
2. Перейдите на закладку **Параметры** (см. рис. 109), из раскрывающегося списка в верхней части окна выберите значение **Сервис**.

На закладке **Сервис** в блоке **Вид** вы можете включать/ отключать интерактивный режим работы Антивируса Касперского на удаленном компьютере: отображение значка Антивируса Касперского в системной панели, вывод уведомлений о возникновении событий в работе приложения (например, обнаружение опасного объекта).

Если флажок **Разрешать взаимодействие с интерфейсом** установлен, пользователь, работающий на удаленном компьютере, будет видеть значок Антивируса, всплывающие сообщения, а также будет иметь возможность принимать решение о дальнейших действиях в окнах уведомлений о наступлении какого-либо события. Для отключения интерактивного режима работы приложения снимите флажок.

В окне, открывающемся по кнопке **Настройка**, на закладке **Собственная информация поддержки** вы можете редактировать информацию о технической поддержке пользователей, которая представлена в разделе **Сервис** пункта **Поддержка** Антивируса Касперского (см. рис. 97).

Для изменения информации в верхнем поле введите актуальный текст о предоставляемой поддержке. В поле ниже вы можете редактировать гиперссылки, которые отображаются в блоке **Техническая поддержка онлайн**, вызываемом при выборе в разделе **Сервис** пункта **Поддержка**.

Редактирование списка осуществляется с помощью кнопок **Добавить**, **Изменить**, **Удалить**. Антивирус Касперского добавляет новую ссылку в начало списка. Для изменения порядка следования ссылок в списке воспользуйтесь кнопками **Вверх**/ **Вниз**.

Если окно не содержит никаких данных, значит информация о технической поддержке, прописанная по умолчанию, редактированию не подлежит.

20.2. Управление задачами

В данном разделе приведена информация об управлении задачами для Антивируса Касперского 6.0 для Windows Workstations. Подробнее о концепции управления задачами через Kaspersky Administration Kit 6.0 смотрите Руководство администратора по данному продукту.

При установке приложения для каждого компьютера сети формируется набор системных задач. В этот список (см. рис. 110) входят задачи защиты (Файловый Антивирус, Веб-Антивирус, Почтовый Антивирус, Проактивная защита, Анти-Шпион, Анти-Хакер), ряд задач поиска вирусов (Проверка Моего Компьютера, Проверка объектов автозапуска, Проверка критических областей) и задачи обновления (обновление сигнатур угроз и модулей приложения, откат обновления).

Вы можете управлять запуском системных задач, настраивать их параметры. Удаление данных задач невозможно.

Кроме того, вы можете создавать собственные задачи, например, задачи поиска вирусов, обновления приложения и отката обновления, задача установки лицензионного ключа (см. п. 20.2.2 на стр. 319).

Для того чтобы просмотреть список задач, сформированных для клиентского компьютера:

1. В папке **Группы** (см. рис. 106) выберите папку с названием группы, в состав которой входит клиентский компьютер.
2. В панели результатов выберите компьютер, для которого вам необходимо создать локальную задачу, и воспользуйтесь командой **Задачи** контекстного меню или аналогичным пунктом в меню **Действие**. В результате откроется окно просмотра свойств клиентского компьютера.
3. На закладке **Задачи** (см. рис. 110) представлен полный перечень задач, сформированных для данного клиентского компьютера.

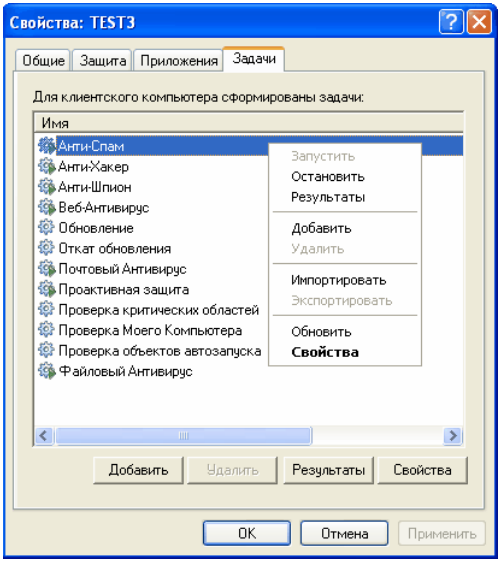


Рисунок 110. Список задач Антивируса Касперского

20.2.1. Запуск и остановка задач

Запуск задач на компьютере выполняется только в том случае, если запущено соответствующее приложение (см. п. 20.1.1 на стр. 312). При остановке приложения выполнение запущенных задач прекращается.

Запуск и остановка задач осуществляется автоматически (в соответствии с расписанием) или вручную (при помощи команд контекстного меню), а также из окна просмотра настроек задачи. Вы можете приостановить процесс выполнения запущенной задачи и возобновить его.

Для того чтобы запустить / остановить / приостановить / возобновить действие задачи вручную,

выберите необходимую задачу, откройте контекстное меню и выберите команду **Запустить / Остановить/ Приостановить / Возобновить** или воспользуйтесь аналогичными пунктами в меню **Действие**.

Аналогичные операции вы можете инициировать из окна настройки задачи на закладке **Общие** (см. рис. 111) при помощи одноименных кнопок.

20.2.2. Создание задач

При работе с Антивирусом Касперского через Kaspersky Administration Kit вы можете создавать:

- локальные задачи – определяются для отдельного клиентского компьютера;
- групповые задачи – определяются для группы клиентских компьютеров;
- глобальные задачи – определяются для набора клиентских компьютеров из произвольных групп логической сети.

Вы можете вносить изменения в параметры задач, наблюдать за их выполнением, копировать и переносить задачи из одной группы в другую, а также удалять при помощи стандартных команд контекстного меню **Копировать/Вставить**, **Вырезать/Вставить** и **Удалить** или аналогичных пунктов в меню **Действие**.

20.2.2.1. Создание локальной задачи

Чтобы создать задачу для отдельного клиентского компьютера, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера на закладке **Задачи** (см. рис. 110).
2. Воспользуйтесь кнопкой **Добавить** для добавления новой задачи. В результате будет открыть окно создания новой задачи, ее интерфейс выполнен в стиле программы-мастера Microsot Windows и состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера при помощи кнопки **Готово**. Для прекращения работы программы на любом этапе служит кнопка **Отмена**.

Шаг 1. Ввод общих данных о задаче

Первое окно мастера является вводным: здесь необходимо указать имя задачи (поле **Имя**).

Шаг 2. Выбор приложения и типа задачи

На данном этапе вам необходимо указать приложение, для которого создается задача, – Антивирус Касперского 6.0 для Windows Workstations. А так-

же выбрать тип задачи. Для Антивируса Касперского 6.0 возможно создание следующих задач:

- *Поиск вирусов* – задача поиска вирусов в указанных пользователем областях.
- *Обновление* – задача получения и применения пакета обновлений для приложения.
- *Откат обновления* – задача отката последнего произведенного обновления приложения.
- *Установка лицензионного ключа* – задача добавления нового лицензионного ключа для работы приложения.

Шаг 3. Настройка параметров выбранного типа задачи

В зависимости от выбранного на предыдущем шаге типа задачи содержимое следующих окон варьируется:

ПОИСК ВИРУСОВ

В окне настройки задачи поиска вирусов требуется указать действие, которое будет выполнять Антивирус Касперского при обнаружении опасного объекта (см. п. 14.4.4 на стр. 215), а также сформировать список объектов проверки (см. п. 14.2 на стр. 206).

ОБНОВЛЕНИЕ

Для задачи обновления сигнатур угроз и модулей приложения требуется указать источник, из которого будут загружены обновления (см. п. 16.4.1 на стр. 229). По умолчанию обновление выполняется с сервера обновлений приложения Kaspersky Administration Kit.

ОТКАТ ОБНОВЛЕНИЯ

Задача отката последнего произведенного обновления не имеет специфических настроек.

УСТАНОВКА ЛИЦЕНЗИОННОГО КЛЮЧА

Для задачи добавления лицензионного ключа с помощью кнопки **Обзор** укажите путь к файлу ключа. Для того чтобы сделать добавляемый ключ резервным установите флажок **Добавить как резервный ключ**. Резервный лицензионный ключ становится активным по окончании срока действия текущего лицензионного ключа.

Информация о добавленном ключе (номер лицензии, тип и дата окончания) представлена в поле ниже.

Шаг 4. Настройка запуска задачи от имени другой учетной записи

На данном шаге вам предлагается настроить запуск задачи от имени учетной записи пользователя, обладающего достаточными правами доступа к объекту проверки или источнику обновления (подробнее см. п. 6.4 на стр. 88).

Шаг 5. Настройка расписания

По завершении настройки параметров задач вам предлагается настроить расписание автоматического запуска задачи.

Для этого из раскрывающегося списка выберите периодичность запуска задачи и в нижней части окна уточните параметры расписания.

Шаг 6. Завершение создания задачи

В последнем окне мастер проинформирует вас об успешном завершении процесса создания задачи.

20.2.2.2. Создание групповой задачи

Чтобы создать групповую задачу для Антивируса Касперского, выполните следующие действия:

1. В дереве консоли выберите группу, для которой вы будете создавать задачу.
2. Выберите входящую в ее состав папку **Групповые задачи** (см. рис. 106), вызовите контекстное меню и выберите команду **Создать → Задачу** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер создания задачи, аналогичный мастеру создания локальной задачи (подробнее см. п. 20.2.2.1 на стр. 319). Следуйте его указаниям.

По окончании работы мастера задача будет добавлена в папку **Групповые задачи** соответствующей группы, всех входящих в ее состав вложенных групп и представлена в панели результатов.

20.2.2.3. Создание глобальной задачи

Чтобы создать глобальную задачу для Антивируса Касперского, выполните следующие действия:

1. Выберите в дереве консоли узел **Глобальные задачи** (см. рис. 106), вызовите контекстное меню и выберите команду **Создать → Задачу** или воспользуйтесь аналогичным пунктом в меню **Действие**.
2. В результате запускается мастер создания задачи, аналогичный мастеру создания локальной задачи (подробнее см. п. 20.2.2.1 на стр. 319). Исключение составляет наличие этапа определения списка клиентских компьютеров из состава логической сети, для которых формируется глобальная задача.
3. Выберите компьютеры из состава логической сети, на которых будет запускаться задача. Можно выбрать компьютеры из разных папок, можно выбрать сразу всю папку (подробнее см. Руководство администратора «Kaspersky Administration Kit 6.0»).

Глобальные задачи выполняются только для заданного набора компьютеров. Если в состав группы, для компьютеров которой сформирована задача удаленной установки, будут добавлены новые клиентские компьютеры, для них данная задача выполняться не будет. Необходимо создать новую задачу или внести соответствующие изменения в настройки существующей.

По окончании работы мастера сформированная глобальная задача будет добавлена в состав узла **Глобальные задачи** дерева консоли и представлена в панели результатов.

20.2.3. Настройка параметров задач

Для просмотра или изменения параметров задач клиентского компьютера:

1. Откройте окно свойств клиентского компьютера на закладке **Задачи** (см. рис. 110).
2. Выберите задачу в списке и воспользуйтесь кнопкой **Свойства**. В результате будет открыто окно настройки параметров задачи (см. рис. 111).

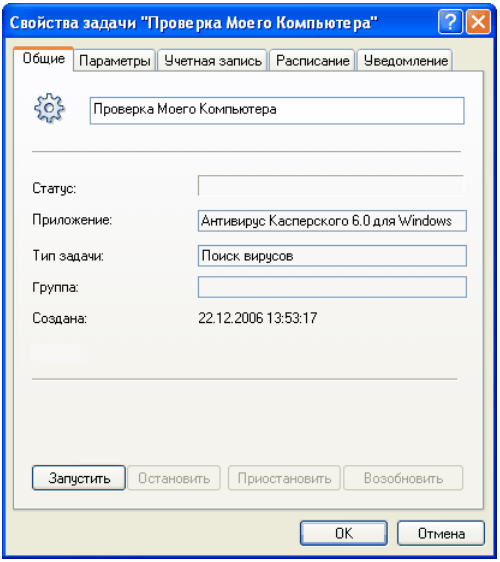


Рисунок 111. Настройка параметров задачи

Все закладки (кроме закладки **Параметры**) являются стандартными для приложения Kaspersky Administration Kit 6.0, их подробное описание смотрите в одноименном Руководстве администратора. Закладка **Параметры** содержит специфические параметры Антивируса Касперского, содержимое данной закладки варьируется в зависимости от выбранного типа задачи.

Настройка параметров задач приложения через интерфейс Kaspersky Administration Kit аналогична настройке через локальный интерфейс Антивируса Касперского, за исключением параметров, которые настраиваются индивидуально для каждого пользователя, например, «черные» и «белые» списки Анти-Спама. Подробное описание настройки параметров задач смотрите в разделах Глава 7 – Глава 16 на стр. 94 – 225 текущей документации.

Если для приложения создана политика (см. п. 20.3 на стр. 323), в которой запрещено переопределение некоторых параметров, то их изменение при настройке задач будет недоступно.

20.3. Управление политиками

Определение политик позволяет распространять единые настройки параметров приложения и задач на клиентские компьютеры, входящие в состав одной группы логической сети.

В данном разделе приведена информация о создании и настройке политики для Антивируса Касперского 6.0 для Windows Workstations. Подробнее о концепции управления политиками через Kaspersky Administration Kit 6.0 смотрите Руководство администратора по данному продукту.

20.3.1. Создание политики

Чтобы создать политику для Антивируса Касперского 6.0, выполните следующие действия:

1. В дереве консоли в папке **Группы** (см. рис. 106) выберите группу компьютеров, для которой планируется создать политику.
2. Выберите входящую в состав выбранной группы папку **Политики**, откройте контекстное меню и воспользуйтесь командой **Создать → Политику**.
   Интерфейс программы создания политики выполнен в стиле программы-мастера для Microsoft Windows и состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

При настройке политики вы можете накладывать запрет на полное или частичное изменение ее параметров в политиках вложенных групп, параметрах задач и параметрах приложения. Для этого нажмите на кнопку  . Для параметров, запрещенных к изменению, она должна принять вид  .

Шаг 1. Ввод общих данных о политике

Первые окна мастера являются вводными. Здесь необходимо указать имя политики (поле **Имя**) и выбрать приложение **Антивирус Касперского 6.0 для Windows Workstations** из раскрывающегося списка **Имя приложения**.

Шаг 2. Выбор статуса политики

В данном окне вам предлагается указать статус политики, для этого установите переключатель в нужное положение: активная политика или неактивная политика.

В группе для одного приложения может быть создано несколько политик, но действующей (активной) политикой может быть только одна из них.

Шаг 3. Выбор и настройка компонентов защиты

На данном этапе вы можете включать/ отключать, а также настраивать компоненты защиты, которые будут использоваться в политике.

По умолчанию все компоненты защиты включены. Для того чтобы отключить какой-либо из компонентов, снимите флажок рядом с его названием. Для детальной настройки компонента защиты выберите его в списке и нажмите на кнопку **Настройка**.

Шаг 4. Настройка параметров поиска вирусов

На данном этапе вам предлагается настроить параметры, которые будут использоваться задачами поиска вирусов.

В блоке **Уровень безопасности** выберите один из трех предопределенных уровней безопасности (см. п. 14.4.1 на стр. 210). Для детальной настройки выбранного уровня воспользуйтесь кнопкой **Настройка**. Для восстановления параметров **Рекомендуемого** уровня защиты воспользуйтесь кнопкой **По умолчанию**.

В блоке **Действие** укажите действие, которое должно быть выполнено Антивирусом при обнаружении опасного объекта (см. п. 14.4.4 на стр. 215).

Шаг 5. Настройка параметров обновления

В данном окне вам предлагается настроить параметры обновления Антивируса Касперского.

В блоке **Параметры обновления** укажите предмет обновления (см. п. 16.4.2 на стр. 232). В окне, открывающемся по кнопке **Настройка**, задайте параметры локальной сети (см. п. 16.4.3 на стр. 234) и укажите источник обновления (см. п. 16.4.1 на стр. 229).

В блоке **Действия после обновления** включите / отключите проверку карантинного хранилища после получения нового пакета обновлений (см. п. 16.4.4 на стр. 236).

Шаг 6. Применение политики

На данном этапе вам предлагается выбрать способ распространения политики на клиентские компьютеры группы (подробнее смотрите Руководство администратора “Kaspersky Administration Kit 6.0”).

Шаг 7. Завершение создания политики

Последнее окно мастера проинформирует вас об успешном завершении процесса создания политики.

По окончании работы мастера политика для заданного приложения будет добавлена в папку **Политики** (см. рис. 106) соответствующей группы и представлена в панели результатов.

Для созданной политики вы можете отредактировать ее настройки и установить ограничения на изменения ее параметров с помощью кнопки для каждой группы настроек. Пользователь на клиентском компьютере не сможет изменить настройки, зафиксированные таким образом. Распространение политики на клиентские компьютеры будет осуществлено при первой синхронизации клиентов с сервером.

Вы можете копировать и переносить политики из одной группы в другую, удалять при помощи стандартных команд контекстного меню **Копировать / Вставить**, **Вырезать / Вставить** и **Удалить** или аналогичных пунктов в меню **Действие**.

20.3.2. Просмотр и редактирование параметров политики

На этапе редактирования вы можете вносить изменения в политику, накладывать запрет на изменение параметров в политиках вложенных групп, в параметрах приложения и параметрах задач.

Для просмотра и редактирования параметров политики:

1. В дереве консоли в папке **Группы** выберите группу компьютеров, для которой вы собираетесь отредактировать параметры политики.
2. Выберите входящую в состав данной группы папку **Политики** (см. рис. 106), при этом в панели результатов будут отображены все политики, созданные для группы.
3. В списке политик выберите политику для приложения **Антивирус Касперского 6.0 для Windows Workstations** (название приложения указано в поле **Приложение**).
4. Откройте контекстное меню выбранной политики и воспользуйтесь командой **Свойства**. На экране появится окно настройки политики для Антивируса Касперского 6.0 (см. рис. 112).

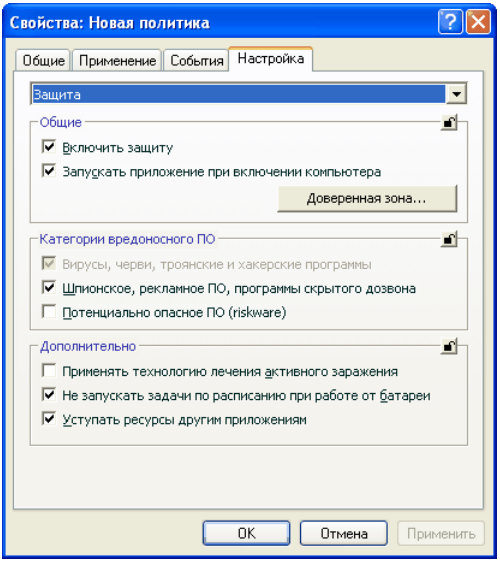


Рисунок 112. Настройка параметров политики

Все закладки (кроме **Настройка**) являются стандартными для приложения Kaspersky Administration Kit 6.0, их подробное описание смотрите в одноименном Руководстве администратора.

На закладке **Настройка** представлены параметры политики для Антивируса Касперского 6.0. Параметры политики включают в себя параметры приложения (см. п. 20.1.2 на стр. 313) и параметры задач (см. п. 20.2.3 на стр. 322).

Дла настройки параметров из раскрывающегося списка в верхней части окна выберите нужное значение и произведите настройку.

ГЛАВА 21. 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 6.0 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: зачем нужен файл ключа? Может ли Антивирус Касперского работать без него?

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. В главном окне приложения воспользуйтесь ссылкой Настройка и в окне настройки приложения выберите раздел **Защита**.
5. Снимите флажок **Запускать приложение при включении компьютера** и нажмите на кнопку **ОК**.
6. Перезагрузите операционную систему в обычном режиме.

После этого обратитесь в Службу технической поддержки через веб-сайт «Лаборатории Касперского» (раздел **Сервис → Техподдержка → Отправить запрос в поддержку**). 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 также представлена информация о параметрах файла setup.ini, использующегося при установке приложения в скрытом режиме.

А.1. Список объектов, проверяемых по расширению

Если в качестве объектов проверки Файлового Антивируса или задачи поиска вирусов вы выбрали вариант **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 объектов, присоединенных к почтовому сообщению:

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, например: *doc* – документ Microsoft Office Word, *docx* – документ Microsoft Office Word 2007 с поддержкой языка XML, *docm* – документ Microsoft Office Word 2007 с поддержкой макросов.

*dot** – шаблон документа Microsoft Office Word, например, *dot* – шаблон документа Microsoft Office Word, *dotx* – шаблон документа Microsoft Office Word 2007, *dotm* – шаблон документа Microsoft Office Word 2007 с поддержкой макросов.

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 метафайла 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: *xla* – расширение Microsoft Office Excel, *xlc* – диаграмма, *xlt* – шаблон документов, *xlsx* – рабочая книга Microsoft Office Excel 2007, *xltm* – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, *xlsb* – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, *xltx* – шаблон Microsoft Office Excel 2007, *xlsm* – шаблон Microsoft Office Excel 2007 с поддержкой макросов, *xlam* – надстройка Microsoft Office Excel 2007 с поддержкой макросов.

*pp** – документы и файлы Microsoft Office PowerPoint, такие как: *pps* – слайд Microsoft Office PowerPoint, *ppt* – презентация, *pptx* – презентация Microsoft Office PowerPoint 2007, *pptm* – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, *potx* – шаблон презентации Microsoft Office PowerPoint 2007, *potm* – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, *ppsx* – слайд-шоу Microsoft Office PowerPoint 2007, *ppsm* – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, *ppam* – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов.

*md** – документы и файлы Microsoft Office Access, такие как: *mda* – рабочая группа Microsoft Office Access, mdb – база данных и т.д.

sldx – слайд Microsoft Office PowerPoint 2007.

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов.

thmx – тема Microsoft Office 2007.

Помните, что фактический формат файла может не совпадать с форматом, указанном в расширении файла.

A.2. Разрешенные маски исключений файлов

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

- 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*
- Маски с абсолютными путями к файлам:
    - **C:\dir*.*** или **C:\dir*** или **C:\dir** – все файлы в каталоге *C:\dir*
    - **C:\dir*.exe** – все файлы с расширением *exe* в каталоге *C:\dir*
    - **C:\dir*.ex?** – все файлы с расширением *ex?* в каталоге *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 подкаталогах указанного каталога, при создании маски установите флажок ☑ **Включая вложенные папки**.
- Маски с относительными путями к файлам:
    - **dir*.*** или **dir*** или **dir** – все файлы во всех каталогах *dir*
    - **dir\test** – все файлы *test* в каталогах *dir*
    - **dir*.exe** – все файлы с расширением *exe* во всех каталогах *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 подкаталогах указанного каталога, при создании маски установите флажок ☑ **Включая вложенные папки**.

Совет.

Использовать маски исключения ***.*** или * допустимо только при указании классификации исключаемой угрозы согласно Вирусной энциклопедии. В этом случае указанная угроза не будет обнаруживаться во всех объектах. Использование данных масок без указания классификации равносильно отключению защиты.

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.

A.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.

A.4. Описание параметров файла *setup.ini*

Файл *setup.ini*, расположенный в каталоге дистрибутива Антивируса Касперского, используется при установке приложения в неинтерактивном режиме через командную строку (см. п. 3.3 на стр. 50) или Редактор объектов групповой политики (см. п. 3.4 на стр. 51). Данный файл содержит следующие параметры:

[Setup] – общие параметры установки приложения.

InstallDir=<путь к каталогу установки приложения>.

Reboot=yes|no – следует ли выполнять перезагрузку компьютера по завершении установки приложения (по умолчанию перезагрузка не выполняется).

SelfProtection=yes|no – следует ли включать самозащиту Антивируса Касперского при установке (по умолчанию самозащита включена).

[Components] – выбор компонентов приложения для установки. В случае если не указан ни один компонент, приложение устанавливается полностью. Если указан хотя бы один из компонентов, неперечисленные компоненты не устанавливаются.

FileMonitor=yes|no – установка компонента Файловый Антивирус.

MailMonitor=yes|no – установка компонента Почтовый Антивирус.

WebMonitor=yes|no – установка компонента Веб-Антивирус.

ProactiveDefence=yes|no – установка компонента Проактивная защита.

AntiSpy=yes|no – установка компонента Анти-Шпион.

AntiHacker=yes|no – установка компонента Анти-Хакер.

AntiSpam=yes|no – установка компонента Анти-Спам.

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

ScanMyComputer=yes|no – задача полной проверки компьютера.

ScanStartup=yes|no – задача проверки объектов автозапуска.

ScanCritical=yes|no – задача проверки критических областей.

Updater=yes|no – задача обновления сигнатур угроз и модулей приложения.

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

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 «C») 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. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие 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.

Антивирус Касперского® 7.0

Антивирус Касперского 7.0 предназначен для защиты персонального компьютера от вредоносных программ, оптимально сочетая в себе традиционные методы защиты от вирусов с новыми проактивными технологиями.

Программа позволяет осуществлять комплексную антивирусную проверку, включающую 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, а также проверку и лечение почтовых баз;
- антивирусную проверку интернет-трафика, поступающего по HTTP-протоколу, в режиме реального времени;
- антивирусную проверку любых отдельных файлов, папок и дисков. Также, используя предустановленную задачу проверки, можно запустить анализ на присутствие вирусов только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows.

Возможности проактивной защиты включают в себя:

- *Контроль изменений в файловой системе*. Программа позволяет создавать список приложений, компонентный состав которых будет контролироваться. Это помогает предотвратить нарушение целостности приложений вредоносными программами.

- *Наблюдение за процессами в оперативной памяти*. Антивирус Касперского 7.0 своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых процессов, а также в случае несанкционированного изменения активных процессов.

- *Мониторинг изменений в реестре операционной системы* благодаря контролю состояния системного реестра.

- *Контроль скрытых процессов* позволяет бороться с сокрытием вредоносного кода в операционной системе с использованием технологий rootkit.

- *Эвристический анализатор.* При проверке какой-либо программы анализатор эмулирует ее исполнение и протоколирует все ее подозрительные действия, например, открытие или запись в файл, перехват векторов прерываний и т.д. На основе этого протокола принимается решение о возможном заражении программы вирусом. Эмуляция происходит в искусственной изолированной среде, что исключает возможность заражения компьютера.

- *Восстановление системы* после вредоносного воздействия программ-шпионов за счет фиксации всех изменений реестра и файловой системы компьютера и их отката по решению пользователя.

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 опе-

ративной памяти компьютера, предотвращает опасные 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. Компонент *Родительский контроль* обеспечивает контроль доступа пользователей компьютера к интернет-ресурсам.

Kaspersky Internet Security 7.0 *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) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Экстренная круглосуточная помощь:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Поддержка пользователей персональных и бизнес-продуктов:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (с 10 до 19 часов) http://support.kaspersky.ru/helpdesk.html
Поддержка корпоративных пользователей:	контактная информация предоставляется при покупке корпоративных продуктов 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) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
Общая информация:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru