ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского 6.0 для Windows Servers

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

АНТИВИРУС КАСПЕРСКОГО 6.0
ДЛЯ WINDOWS SERVERS

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 деятельности человека, проявления. Исходя из этого, все источники угроз можно разделить на три группы:

- **Человеческий фактор**. Данная группа угроз связана с действиями человека, имеющего санкционированный или несанкционированный доступ к информации. Угрозы этой группы можно разделить на:
    - *внешние*, к ним относятся действия кибер-преступников, хакеров, интернет-мошенников, недобросовестных партнеров, криминальных структур.
    - *внутренние*, к ним относятся действия персонала компаний. 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 ин-

формацией. 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 сервере, включая изменение системного реестра, кражу личных данных и установку вредоносного программного обеспечения.

Используя сетевые технологии, злоумышленники реализуют атаки на 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.

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.

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 сервере, а также распространить вирус на другие диски сервера или компьютеры сети.

1.3. Виды угроз

В настоящее время существует огромное количество угроз, которым может подвергнуться сервер. 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 сервере 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 сервере;
- сбор информации о качестве связи, способе подключения, скорости модема и т.д.

Потенциально опасные приложения (Riskware)

Программное обеспечение, которое не имеет какой-либо вредоносной функции, но может быть использовано злоумышленниками в качестве вспомогательных компонентов вредоносной программы, поскольку содержит бреши и ошибки. При некоторых условиях наличие таких программ на компьютере подвергает данные риску. К таким программам относятся, например, 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.

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 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 сервере 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.

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.

ГЛАВА 2. АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS SERVERS

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

2.1. Что нового в Антивирусе Касперского 6.0 для Windows Servers

Рассмотрим детально нововведения Антивируса Касперского 6.0 для Windows Servers.

Новое в защите

- Изменилась технология защиты файлов: 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 сервере. Проверка может занимать достаточное количество времени и ресурсов системы, но администратор 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 сервера, заражение которых может привести к серьезным последствиям, представлена отдельной задачей. Вы можете настроить автоматический запуск этой задачи каждый раз при старте системы.
- Расширена функция оповещения пользователя (см. п. 11.8.1 на стр. 141) 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.

- Добавлена технология самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, защита файлов приложения от несанкционированного доступа и изменения, а также защиты доступа к параметрам приложения с помощью пароля. Это позволяет избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.

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.

- 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 6.0 для Windows Servers

Защита Антивируса Касперского включает:

- Файловый Антивирус (см. п. 2.2.1 на стр. 17), обеспечивающий контроль над объектами файловой системы компьютера в режиме реального времени.
- Задачи поиска вирусов (см. п. 2.2.2 на стр. 18), посредством которых выполняется проверка сервера или отдельных файлов, папок, дисков или областей, на присутствие вирусов.
- Сервисные функции (см. п. 2.2.3 на стр. 18), обеспечивающие информационную поддержку в работе с приложением и позволяющие расширить его функциональность.

2.2.1. Файловый Антивирус

Защита сервера в реальном времени обеспечивается с помощью **Файлового Антивируса**.

Файловая система может содержать вирусы и другие опасные программы. Вредоносные программы могут годами храниться в 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 сервере 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. 11.2 на стр. 124) или помещена на карантин (см. п. 11.1 на стр. 120).

2.2.2. Задачи поиска вирусов

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

Для поиска вирусов в состав Антивируса Касперского 6.0 для Windows Servers 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 сервера.

Мой Компьютер

Поиск вирусов на сервере 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.

2.2.3. Сервисные функции приложения

Антивирус Касперского 6.0 для Windows Servers 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 уничтожить вирус или другую опасную программу, необходимо поддерживать Антивирус Касперского 6.0 для Windows Servers 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 и 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 Файловому Антивирусу, 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 любой составляющей 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 Антивируса Касперского переносит в специальное хранилище – *Карантин*. Здесь они хранятся в зашифрованном виде, чтобы избежать заражения сервера. 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 сервера.

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

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 поддержки онлайн 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, компьютер должен удовлетворять следующим минимальным требованиям.

Общие требования:

- 50 MB свободного места на жестком диске.
- CD-ROM (для установки Антивируса Касперского 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.

Операционная система:

- Microsoft Windows 2000 Server/Advanced Server Service Pack 4 или выше, все текущие обновления.
- Microsoft Windows NT Server 4.0 Service Pack 6a.
- Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003, все Service Packs, все текущие обновления.
- Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition.

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 ДЛЯ WINDOWS SERVERS

Антивирус Касперского 6.0 для Windows Servers 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. 24), данный режим требует участия пользователя в процессе установки;
    - неинтерактивном, запуск установки приложения в данном режиме выполняется из командной строки с применением параметров по умолчанию и не требует участия пользователя в процессе установки (см. п. 3.3 на стр. 34).
- 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. 35).

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. 37). 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 сервер, 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 сервере выполняется проверка соответствия установленных операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки Антивируса Касперского. Также проверяется наличие на сервере 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 сервер.

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 сервере, в который будет установлена приложение. По умолчанию задан путь:

- **<Диск> → Program Files → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Servers** – для 32-разрядных систем.
- **<Диск> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Servers** – 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 или сигнатуры угроз, если таковые были сохранены на сервере при удалении предыдущей версии Антивируса Касперского 6.0.

Рассмотрим подробнее, как включить использование описанных выше возможностей.

Если на сервере ранее была установлена предыдущая версия (сборка) Антивируса Касперского, и при ее удалении вы сохранили на компьютере сиг-

натуры 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 сервер.

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

Шаг 6. Выбор типа установки

На данном этапе вам нужно определить полноту установки приложения на сервер. Предусмотрено два варианта установки:

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

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

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 компонент Файловый Антивирус, 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**.

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. Поиск других антивирусных приложений

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

При обнаружении таких приложений на сервере 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 (автоматически будут удалены только продукты «Лаборатории Касперского»).

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

Шаг 9. Завершающая подготовка к установке приложения

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

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.

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

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

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 10. Завершение процедуры установки

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

Для запуска мастера первоначальной настройки приложения нажмите на кнопку **Далее** (см. п. 3.2 на стр. 28).

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

3.2. Мастер первоначальной настройки

Мастер настройки Антивируса Касперского запускается по завершении процедуры установки приложения. Его задача – помочь вам провести первичную настройку параметров приложения, исходя из особенностей и задач сервера.

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**.

Если вы прервете процедуру первоначальной настройки, закрыв окно мастера, приложение не будет работать. При каждом запуске приложения, мастер первоначальной настройки будет запускаться заново до тех пор, пока процедура первоначальной настройки не будет успешно завершена.

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 файла лицензионного ключа для Антивируса Касперского 6.0.
- **Активировать приложение позже**. При выборе этого варианта этап активации приложения будет пропущен. Антивирус Касперского будет установлен на сервер, 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. 10.4.3 на стр. 114) 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. 11.5 на стр. 135) 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 электронной 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, 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. Настройка параметров обновления

Качество защиты сервера 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**.

3.2.4. Настройка расписания проверки на вирусы

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

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 Server) 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 сервера на вирусы.

3.2.5. Ограничение доступа к приложению

В связи с тем, что сервер может использоваться несколькими людьми, 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.

3.2.6. Завершение работы мастера настройки

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

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

3.3. Процедура установки приложения из командной строки

Для того чтобы установить Антивирус Касперского 6.0 для Windows Servers, наберите в командной строке:

```
msiexec /i <имя_пакета>
```

Будет запущен мастер установки (см. п. 3.1 на стр. 24). 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. 191), конфигурационного файла *install.cfg* (см. п. 13.7 на стр. 179), 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 Server 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. 191), конфигурационный файл *install.cfg* (см. п. 13.7 на стр. 179), 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 вариант установки поверх существующего пакета.

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

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

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 сервере установлено приложение Антивирус Касперского 5.0 для Windows File Servers, вы можете обновить его до Антивируса Касперского 6.0 для Windows Servers.

После запуска программы установки Антивируса Касперского 6.0 вам будет предложено сначала удалить установленную пятую версию продукта. По завершении удаления требуется перезагрузка компьютера, после чего начинается установка приложения версии 6.0.

Внимание!

Если вы устанавливаете Антивирус Касперского 6.0 для Windows Servers из сетевой папки, доступ к которой ограничен с помощью пароля, на предыдущую версию продукта, обратите внимание на следующую особенность. После удаления приложения версии 5.0 и перезагрузки компьютера, программа установки не дает возможность получить доступ к сетевой папке, где расположен дистрибутив приложения. В результате этого установка продукта обрывается. Для корректной установки 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. 38);
- контекстное меню (см. п. 4.2 на стр. 39);
- главное окно (см. п. 4.3 на стр. 40);
- окно настройки параметров приложения (см. п. 4.4 на стр. 42).

4.1. Значок в системной панели

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

Значок является своего рода индикатором работы приложения. Он отражает состояние защиты, а также показывает ряд основных действий, выполняемых приложением.

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

В зависимости от выполняемой операции значок Антивируса Касперского меняется:

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

 выполняется обновление сигнатур угроз и модулей приложения Антивируса Касперского.

 произошел сбой в работе какого-либо компонента Антивируса Касперского.

Также значок обеспечивает доступ к основным элементам интерфейса приложения: контекстному меню (см. п. 4.2 на стр. 39) и главному окну (см. п. 4.3 на стр. 40).

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.

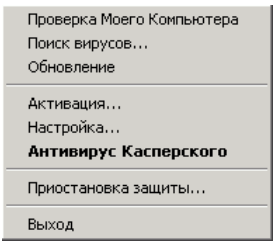


Рисунок 1. Контекстное меню

Меню Антивируса Касперского содержит следующие пункты:

Проверка Моего Компьютера – запуск полной проверки сервера 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 системная память, объекты автозапуска, почтовые базы, все диски сервера и т.д. Вы можете пополнить список, выбрать объекты для проверки и запустить поиск вирусов.

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

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. 40).

Приостановка защиты / **Включение защиты** – выключение на время/включение работы Файлового Антивируса (см. п. 2.2.1 на стр. 17). 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:

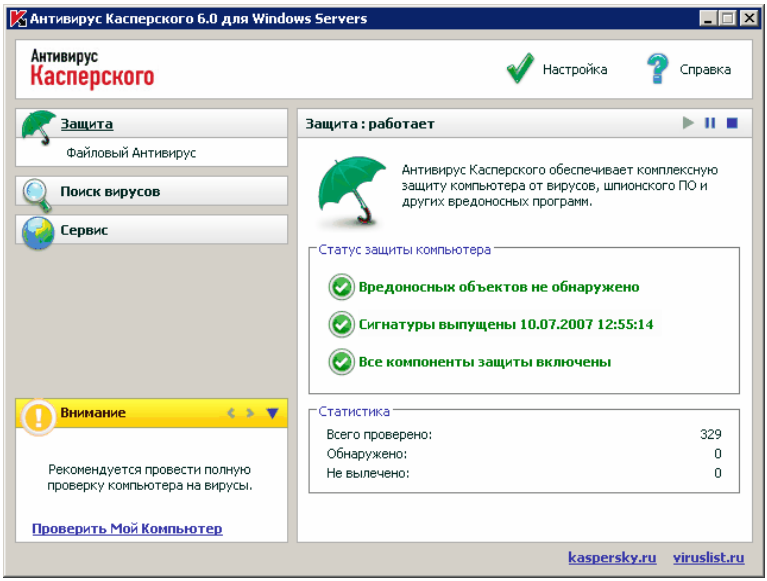
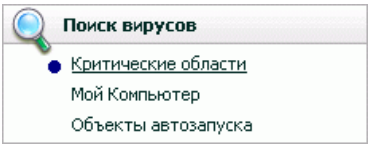
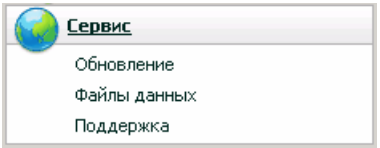


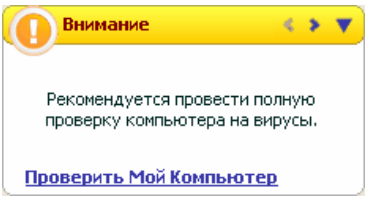
Рисунок 2. Главное окно Антивируса Касперского

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

Выбрав в левой части окна какой-либо раздел, 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 сервера. Раздел **Защита** предназначен именно для этого. 	Чтобы просмотреть общую информацию о работе Антивируса Касперского, ознакомиться с общей статистикой работы приложения, убедиться, все ли корректно работает, выберите в навигационной части раздел **Защита**.
Для проверки сервера 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 сервера.
Раздел **Сервис** включает дополнительные функции Антивируса Касперского. 	Здесь вы можете перейти к обновлению приложения, просмотреть отчеты о работающих и завершенных задачах и компонентах, перейти к работе с объектами на карантине, с резервными копиями, к информации о технической поддержке 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 сервера. 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 Файлового Антивируса и сервисных функций меню содержит пункты, позволяющие быстро перейти к их настройке, к управлению, к просмотру отчета. Для задач поиска вирусов и задач 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. 40). 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 Файлового Антивируса 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.

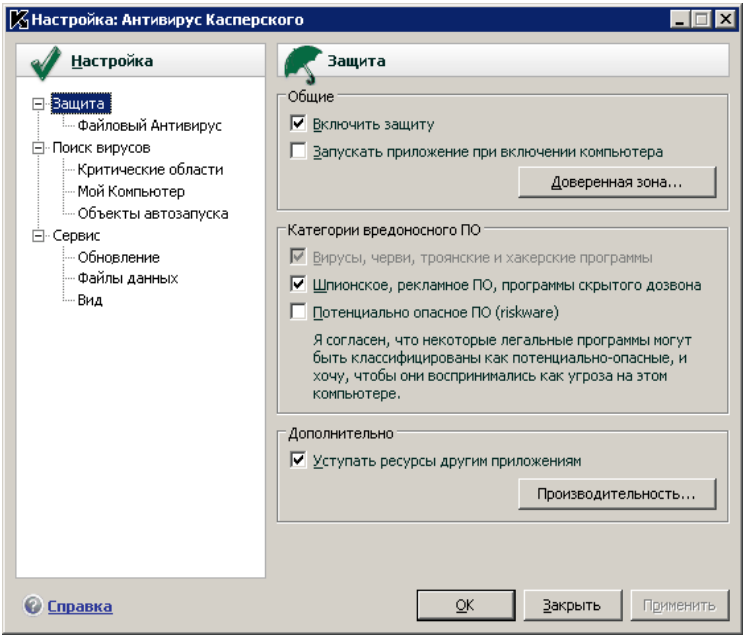


Рисунок 3. Окно настройки Антивируса Касперского

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.

ГЛАВА 5. НАЧАЛО РАБОТЫ

Одной из главных задач специалистов «Лаборатории Касперского» при создании Антивируса Касперского для Windows Servers являлась оптимальная настройка всех параметров приложения.

Для удобства пользователей мы постарались объединить этапы предварительной настройки в едином интерфейсе мастера первоначальной настройки (см. п. 3.2 на стр. 28), который запускается в конце процедуры установки приложения. Следуя указаниям мастера, вы сможете провести активацию приложения, настроить параметры обновления и запуска задач поиска вирусов, ограничить доступ к приложению с помощью пароля.

После завершения установки и запуска приложения на сервере 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. 44).
- Обновить приложение, если это не было сделано с помощью мастера настройки либо автоматически сразу после установки приложения (см. п. 5.5 на стр. 52).
- Проверить сервер на присутствие вирусов (см. п. 5.2 на стр. 50).

5.1. Каков статус защиты сервера

Сводная информация о защите сервера 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 сервера с помощью специальных индикаторов (см. п. 5.1.1 на стр. 44). Статистика (см. п. 5.1.2 на стр. 48) содержит итог текущей работы приложения.

5.1.1. Индикаторы защиты

Статус защиты определяется тремя индикаторами (см. рис. 4), которые отражают степень защиты сервера в данный момент времени и указывают на проблемы в настройке и работе приложения.

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

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

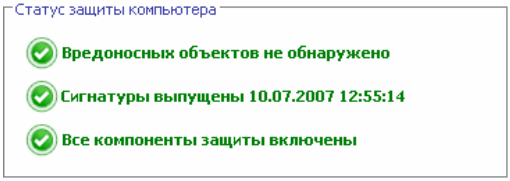


Рисунок 4. Индикаторы, отображающие статус защиты сервера

– *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 сервера. Пожалуйста, строго следуйте рекомендациям, приведенным в разделе комментариев и советов главного окна приложения. Все они направлены на повышение защиты сервера. 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 сервере. Индикатор принимает одно из следующих значений:

Вредоносных объектов не обнаружено

Антивирус Касперского не обнаружил ни одного опасного объекта на сервере.

Все вредоносные объекты обезврежены

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

Обнаружены вредоносные объекты

В данный момент сервер 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 сервера 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 сервера.

Сигнатуры неактуальны

Модули приложения и сигнатуры угроз Антивируса Касперского не обновлялись несколько дней. Вы подвергаете сервер 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 сервере 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 сервер на всех каналах проникновения вредоносных программ.

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 компонента защиты приостановлена на некоторое время. Чтобы возобновить работу компонента выберите пункт **Включение защиты** в контекстном меню, открывающемся при нажатии по значку приложения в системной панели.

Отключены все компоненты защиты

Защита компьютера полностью отключена, не работает компонент защиты. Чтобы возобновить работу компонента выберите пункт **Включение защиты** в контекстном меню, открывающемся при нажатии по значку приложения в системной панели.

Некоторые компоненты защиты неисправны

Произошел сбой в работе компонента 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, 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. В правой части будет представлена сводная информация по работе компонента.

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

Рассмотрим **статусную строку** Файлового Антивируса:

- *Файловый Антивирус : работает* – защита файлов обеспечивается на выбранном уровне (см. п. 7.1 на стр. 73).
- *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».

Параметры, в соответствии с которыми работает компонент, приведены в блоке **Статус**:

- *Файловый Антивирус* – текущий статус компонента (работает, не работает, пауза и т.д.).
- *Уровень безопасности* – набор параметров работы компонента, в соответствии с которыми приложение обеспечивает защиту файлов. По умолчанию используется **Рекомендуемый** уровень безопасности, на котором проверке подвергаются только те объекты файловой системы, которые подвержены заражению. Например, таковыми являются исполняемые (exe) файлы.
- *Действие*, которое выполняется при обнаружении вредоносного объекта.

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.

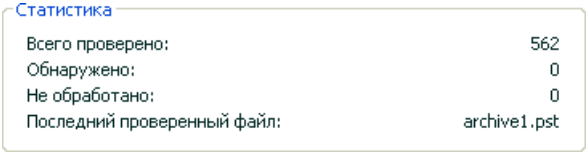


Рисунок 5. Блок общей статистики работы приложения

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. 11.3.2 на стр. 130) и присвоенных им статусах;
- журнал событий (см. п. 11.3.3 на стр. 131);
- общая статистика проверки компьютера (см. п. 11.3.4 на стр. 132);

- параметры работы приложения (см. п. 11.3.5 на стр. 132).

5.2. Как проверить на вирусы сервер

После установки приложение обязательно уведомит вас сообщением в нижней левой части окна приложения о том, что проверка сервера 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 сервера, 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 сервера

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. Выбрать объект для проверки вы можете стандартными средствами операционной системы Microsoft Windows Server (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 Server и выберите пункт **Проверить на вирусы** (см. рис. 6).

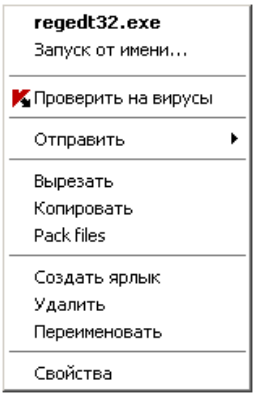


Рисунок 6. Проверка на присутствие вирусов объекта, выбранного средствами Microsoft Windows Server

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 обновить приложение

«Лаборатория Касперского» обновляет сигнатуры угроз и модули приложения 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.

5.6. Что делать, если защита не работает

В случае возникновения проблем или ошибок в работе Файлового Антивируса обязательно обратите внимание на его статус. Если его статус *не работает* или *сбой в работе*, попробуйте перезагрузить приложение.

Если после перезапуска приложения проблема не будет решена, рекомендуется исправить возможные ошибки с помощью программы восстановления приложения (**Пуск → Программы → Антивирус Касперского 6.0 для Windows Servers → Изменение, восстановление или удаление**).

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 Файловый Антивирус 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 о факте запуска и статусе сразу всех компонентов Антивируса Касперского (Файлового Антивируса, 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. 54).
- Определять типы опасных программ, от которых Антивирус Касперского будет защищать сервер (см. п. 6.2 на стр. 59).
- Формировать список исключений из защиты (см. п. 6.3 на стр. 60).
- Создавать собственные задачи поиска вирусов и обновления (см. п. 6.4 на стр. 66).
- Настраивать запуск задач по удобному для вас расписанию (см. п. 6.5 на стр. 68).
- Настраивать параметры производительности (см. п. 6.6 на стр. 70) защиты компьютера.

6.1. Отключение / включение защиты сервера

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 сервер в течение всего сеанса работы. Файловый Антивирус (см. п. 2.2.1 на стр. 17) работает.

Вы можете отключить защиту, обеспечиваемую Антивирусом Касперского.

Внимание!

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

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

6.1.1. Приостановка защиты

Приостановка защиты означает отключение на некоторый промежуток времени Файлового Антивируса.

Для того чтобы приостановить работу Антивируса Касперского,

1. В контекстном меню (см. п. 4.2 на стр. 39) 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. 58).
   - **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.

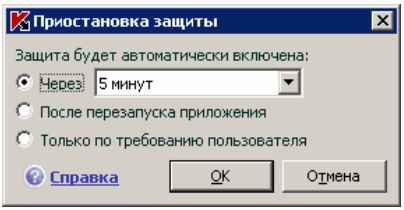


Рисунок 7. Окно приостановки защиты сервера

К вашему сведению.

Отключить защиту сервера можно одним из следующих способов:

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

В результате временного отключения работа Файлового Антивируса приостанавливается. Об этом свидетельствуют:

- Неактивное (серого цвета) имя Файлового Антивируса в разделе **Защита** главного окна.
- Неактивный (серый) значок приложения в системной панели.
- Третий индикатор защиты (см. п. 5.1.1 на стр. 44) сервера, указывающий на то, что **Все компоненты защиты приостановлены**.

6.1.2. Полное отключение защиты сервера

Полное отключение защиты означает остановку работы Файлового Антивируса. Поиск вирусов и обновление продолжают работать в заданном режиме.

Если защита отключена полностью, она может быть включена только по требованию администратора. Автоматического включения Файлового Антивируса после перезагрузки системы или приложения в этом случае не происходит. Помните, что если Антивирус Касперского каким-либо образом конфликтует с другими программами, установленными на сервере, вы можете приостановить работу Файлового Антивируса или сформировать список исключений (см. п. 6.3 на стр. 60).

Чтобы полностью отключить защиту сервера,

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

В результате отключения защиты работа Файлового Антивируса останавливается. Об этом свидетельствуют:

1. Неактивное (серого цвета) имя Файлового Антивируса в разделе **Защита** главного окна.
2. Неактивный (серый) значок приложения в системной панели.
3. Третий индикатор защиты (см. п. 5.1.1 на стр. 44) сервера, указывающий на то, что **Отключены все компоненты защиты**.

6.1.3. Приостановка / отключение компонента защиты или задач

Отключить работу Файлового Антивируса, задачи обновления или поиска вирусов можно несколькими способами. Однако прежде чем делать это, рекомендуем определить причину, по которой вы хотите отключить их. Вероятно, проблему 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. 60).

Чтобы приостановить работу Файлового Антивируса, 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 или задачи,

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

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 сервера

Если в какой-либо момент времени вы приостановили или полностью отключили защиту сервера, 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. 44) 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. 39) приложения. В результате приложение будет выгружено из оперативной памяти, что подразумевает, что сервер на данный период работает в незащищенном режиме.

Если вы завершили работу приложения, включить защиту компьютера снова вы можете, загрузив Антивирус Касперского из меню **Пуск** → **Программы** → **Антивирус Касперского 6.0 для Windows Servers** → **Антивирус Касперского 6.0 для Windows Servers**.

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

Приложение 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 серверу. 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. 42) выберите раздел **Защита**.

Типы угроз (см. п. 1.1 на стр. 10) приведены в блоке **Категории вредоносного ПО**:

- **Вирусы, черви, троянские и хакерские программы**. Эта группа объединяет наиболее распространенные и опасные категории вредоносных программ. Защита от них обеспечивает минимально-допустимый уровень безопасности. В соответствии с рекомендациями специалистов «Лаборатории Касперского» Антивирус Касперского всегда контролирует вредоносные программы данной категории.
- **Шпионское, рекламное ПО, программы скрытого дозвона**. Данная группа объединяет в себе потенциально опасное программное обеспечение, которое может причинить неудобство 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 серверу.

Приведенные группы регулируют полноту использования сигнатур угроз при проверке объектов в режиме реального времени и при поиске вирусов на сервере.

Если выбраны все группы, Антивирус Касперского обеспечивает максимально полную антивирусную защиту сервера. 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 сервере 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. 60).

6.3. Формирование доверенной зоны

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

Доверенную зону формирует администратор, 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**.

В открывшемся окне (см. рис. 8) настройте правила исключений для объектов, а также сформируйте список доверенных приложений.

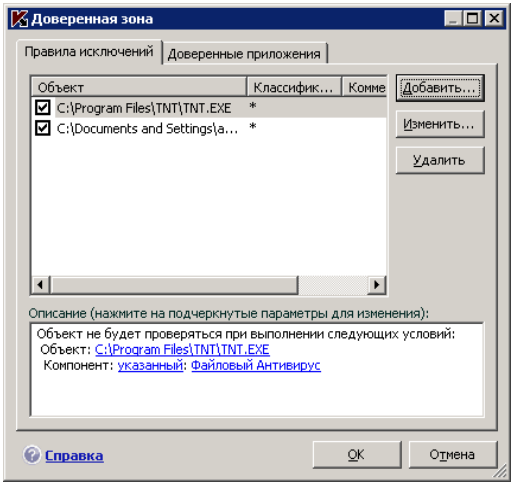


Рисунок 8. Формирование доверенной зоны

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 Файловым Антивирусом, 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**:

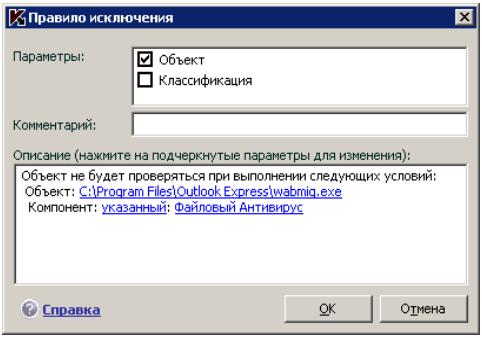


Рисунок 9. Создание правила исключения

- **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.

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. 189). Чтобы указанный объект (файл, маска файла, папка) рекурсивно исключался при проверке, установите флажок ☑ **Включая вложенные папки**.
   - 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. 191).

     Для некоторых объектов по классификации в поле **Дополнительные параметры** можно задать дополнительные условия применения правила.
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 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**.

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. 10).

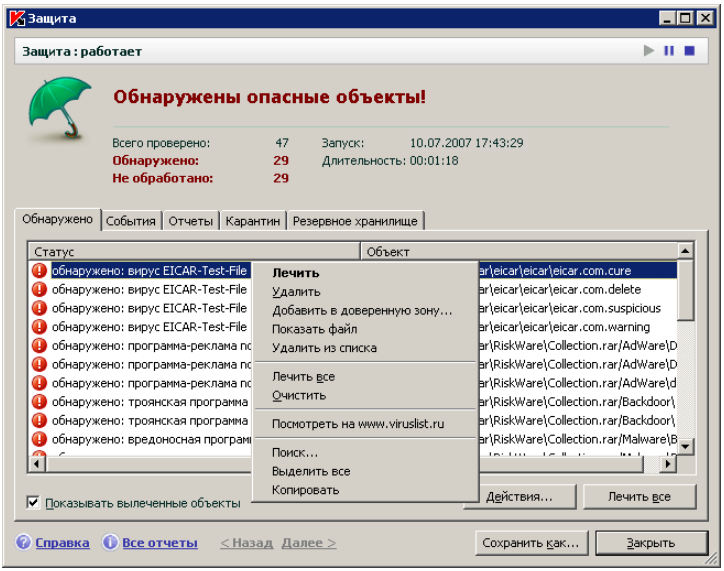


Рисунок 10. Создание правила исключения из отчета

6.3.2. Доверенные приложения

Антивирус Касперского позволяет формировать список доверенных приложений, файловая активность которых не будет контролироваться.

Например, вы считаете объекты, используемые стандартной программой Microsoft Windows Server – **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. 61).

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.

По умолчанию Антивирус Касперского проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом.

Формирование списка доверенных приложений осуществляется на специальной закладке **Доверенные приложения** (см. рис. 11). По умолчанию при установке Анитивируса 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.

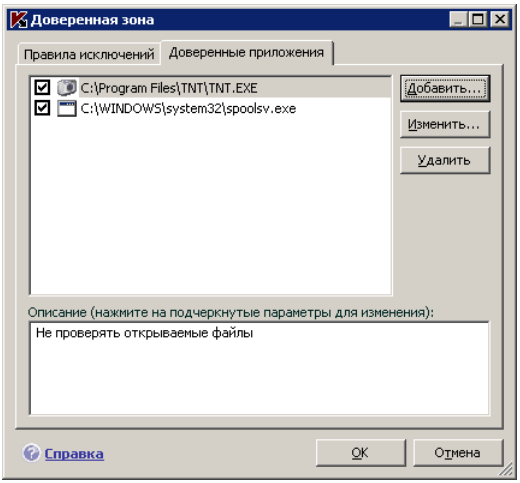


Рисунок 11. Список доверенных приложений

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. 12) 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.

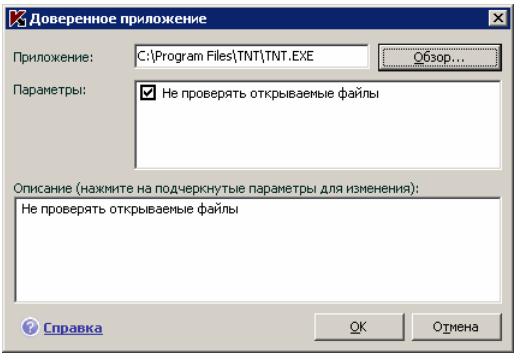


Рисунок 12. Добавление приложения в список доверенных

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.

3. Далее, если необходимо, укажите действие, выполняемое данным процессом, которое не будет контролироваться Антивирусом Касперского:

   Не проверять открываемые файлы – исключать из проверки все файлы, которые открываются процессом доверенного приложения.

6.4. Запуск задач с правами другой учетной записи

В Антивирусе Касперского реализован сервис запуска 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 може-

те настроить запуск задачи от имени другой учетной записи, обладающего такими привилегиями.

Что касается обновления приложения, то оно может производиться из источника, к которому у вас нет доступа (например, к сетевому каталогу обновлений) или прав авторизованного пользователя прокси-сервера. Вы можете воспользоваться данным сервисом, чтобы запускать обновление приложения от имени пользователя, обладающего такими привилегиями.

Чтобы настроить запуск задачи 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. 13).
3. Для включения данного сервиса установите флажок **Запуск задачи от имени**. Ниже введите данные учетной записи, под которой будет запускаться задача: имя пользователя и пароль.

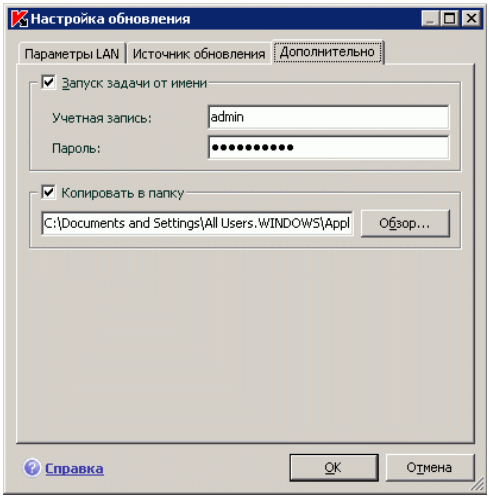


Рисунок 13. Настройка запуска задачи обновления от имени другой учетной записи

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 задач 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. 14), которое открывается по кнопке **Изменить**.

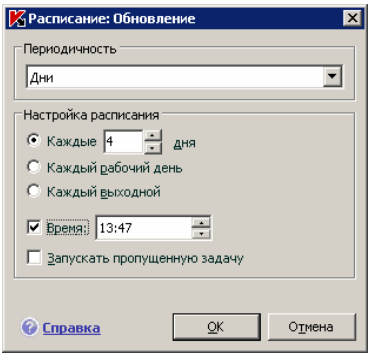


Рисунок 14. Формирование расписания запуска задач

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. 14) требующийся вариант. Далее необходимо указать параметры расписания для выбранного варианта в

блоке **Настройка расписания**. На выбор предлагаются следующие варианты:

- **В определенное время**. Производить запуск задачи или 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).
- **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.

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

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** (см. рис. 15).

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.

В окне, открывающемся по кнопке **Производительность**, вы можете задачть параметры Антивируса Касперского при работе на многопроцессорном сервере (см. п. 6.7 на стр. 70).

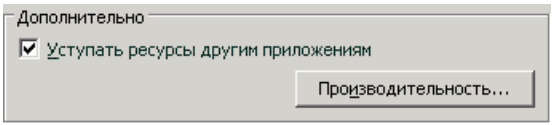


Рисунок 15. Настройка производительности

Чтобы настроить параметры производительности,

выберите раздел **Защита** главного окна приложения и воспользуйтесь ссылкой Настройка. Настройка параметров производительности производится в блоке **Дополнительно**.

6.7. Многопроцессорная конфигурация сервера

В данном окне вы можете настроить параметры производительности работы сервера при использовании многопроцессорной конфигурации.

Количество копий антивирусного ядра – число экземпляров антивирусного ядра, загружаемых при запуске Антивируса Касперского на сервере.

Эта величина определяет число параллельно запущенных антивирусных процессов.

Чем большее количество копий антивирусного ядра запущено, тем быстрее выполняется антивирусная обработка объектов. Однако это сказывается на общей производительности работы сервера.

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

Для автоматического распределения антивирусных процессов между процессорами сервера установите флажок **Использовать специальный драйвер для организации параллельной обработки**.

Если флажок снят, вы можете вручную регулировать нагрузку на сервер, например, часть процессоров зарезервировать под антивирусную обработку объектов, а часть – под непосредственные задачи сервера. Для этого в блоке **Используемые процессоры** снимите флажки с тех процессоров, которые необходимо выделить непосредственно для работы сервера.

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

ГЛАВА 7. АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВОЙ СИСТЕМЫ СЕРВЕРА

В состав Антивируса Касперского входит *Файловый Антивирус*, который обеспечивает защиту файловой системы сервера от заражения. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

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

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

1. Обращение пользователя или некоторой программы к каждому файлу перехватывается компонентом.
2. Файловый Антивирус проверяет наличие информации о перехваченном файле в базе 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 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 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. 16):

- **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.

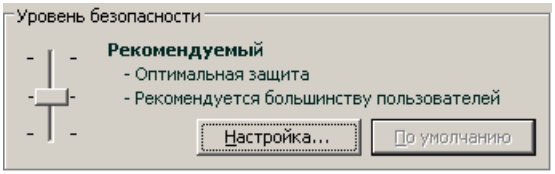


Рисунок 16. Уровни безопасности Файлового Антивируса

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 сервера.

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 сервере, определяется набором параметров. Их можно разбить на следующие группы:

- параметры, определяющие типы файлов, подвергаемые анализу на вирусы (см. п. 7.2.1 на стр. 75);
- параметры, формирующие защищаемую область (см. п. 7.2.2 на стр. 78);
- параметры, задающие действия над опасным объектом (см. п. 7.2.5 на стр. 82);
- дополнительные параметры работы Файлового Антивируса (см. п. 7.2.3 на стр. 79).

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. 17). 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. 187), которые подвергаются проверке в данном случае.

Совет.

Не стоит забывать, что злоумышленник может отправить вирус на сервер 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.

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.

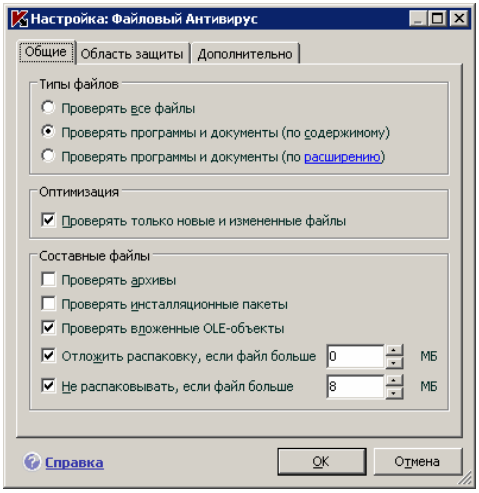


Рисунок 17. Выбор типов файлов, подвергаемых антивирусной проверке

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 Office 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 для работы. Проверка объектов, входящих в его состав, будет произведена позже. Если флажок не установлен, доступ к фай-

лам 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. 18).

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 серверу. Вы можете наполнить или отредактировать список с помощью кнопок **Добавить**, **Изменить**, **Удалить**.

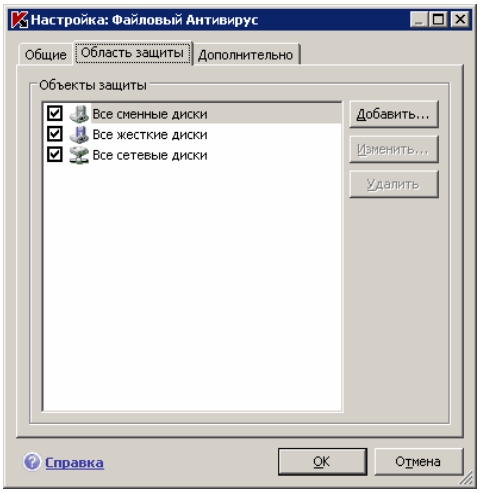


Рисунок 18. Формирование защищаемой области

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. 60).
- Объединить первый и второй способы, то есть сформировать область защиты, из которой исключить ряд объектов.

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 сервера!

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. 19).

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.

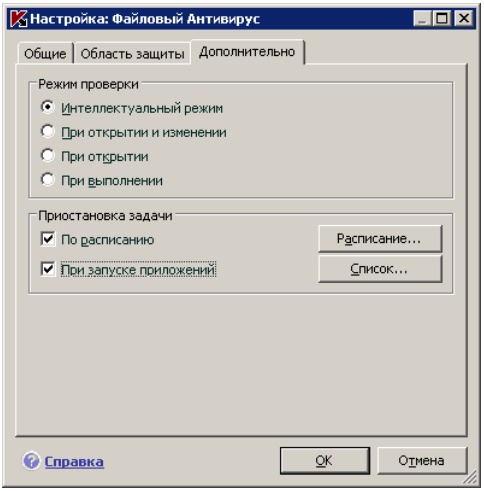


Рисунок 19. Настройка дополнительных параметров Файлового Антивируса

- **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.

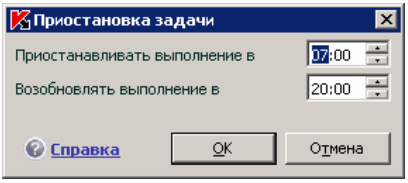


Рисунок 20. Приостановка работы компонента

Для отключения работы компонента при работе с программами, требующими значительных ресурсов, установите флажок ☑ **При запуске приложений** и в окне (см. рис. 21), открывающемся по кнопке **Список**, сформируйте список программ.

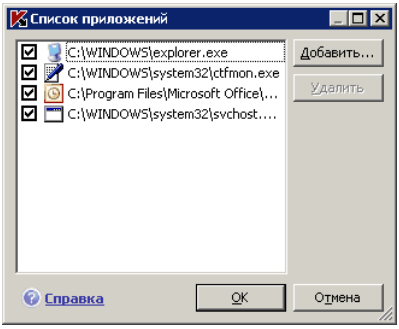


Рисунок 21. Формирование списка приложений

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.

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. 9).
- *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. 22).

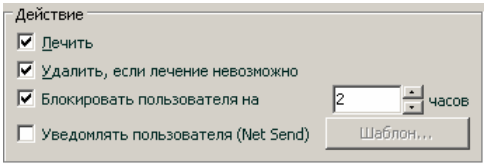


Рисунок 22. Возможные действия Файлового Антивируса над опасным объектом

Если в качестве действия вы выбрали	**При обнаружении опасного объекта**
☑ **Лечить** ☐ **Удалить, если лечение невозможно**	Доступ к объекту блокируется и производится попытка его лечения, при этом копия объекта сохраняется в резервном хранилище. Если объект вылечить удалось, он предоставляется пользователю для работы. Если объект не удалось вылечить, то он помещается на карантин. Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.
☑ **Лечить** ☑ **Удалить, если лечение невозможно**	Доступ к объекту блокируется и производится попытка его лечения, при этом копия объекта сохраняется в резервном хранилище. Если объект вылечить удалось, он предоставляется пользователю для работы. Если объект вылечить не удалось, то он будет удален.
☐ **Лечить** ☑ **Удалить**	Файловый Антивирус блокирует доступ к объекту и удаляет его.
☑ **Блокировать пользователя на … часов**	Заблокировать текущее подключение учетной записи пользователя к серверу при попытке копирования зараженного или возможно зараженного объекта. Данное действие может быть применено дополнительно к действиям, связанным с обработкой объекта –

Если в качестве действия вы выбрали	При обнаружении опасного объекта
	лечению или удалению. Обратите внимание, что если пользователь завершит сеанс работы и снова выполнит вход в систему, это будет расцениваться Антивирусом Касперского как другое подключение и блокировка будет снята.
☑ **Уведомлять пользователя (Net Send)**	Уведомлять пользователя, с компьютера которого была произведена попытка копирования зараженного или возможно зараженного объекта на сервер, по сети Net Send. Для настройки шаблона уведомления воспользуйтесь кнопкой **Шаблон** (см. п. 7.2.6 на стр. 84).

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

Внимание! В приложении, установленном на компьютере под управлением операционной системы Microsoft Windows NT Server 4.0, недоступны действия **Блокировать пользователя** и **Уведомлять пользователя (NetSend)**.

7.2.6. Формирование шаблона уведомления

В данном окне вы можете сформировать текст шаблона уведомления пользователя, с компьютера которого была произведена попытка копирования зараженного/ возможно зараженного объекта на сервер.

Текст уведомления для большей информативности может содержать макросы: путь к опасному объекту и имя угрозы. Для добавления макросов в текст уведомления воспользуйтесь кнопкой **Макрос**.

Для восстановления первоначального текста, используемого в качестве шаблона уведомления, воспользуйтесь кнопкой **По умолчанию**.

7.3. Отложенное лечение объектов

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

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 сервера. Настоятельно не рекомендуется пропускать вредоносные объекты.

ГЛАВА 8. ПОИСК ВИРУСОВ НА СЕРВЕРЕ

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

В состав Антивируса Касперского 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 сервера.

Мой Компьютер

Поиск вирусов на сервере 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. Вы можете изменять эти параметры (см. п. 8.4 на стр. 90), а также устанавливать расписание запуска задач (см. п. 6.5 на стр. 68).

Также предусмотрена возможность создавать собственные задачи (см. п. 8.3 на стр. 89) поиска вирусов и формировать расписание их запуска. Например, можно создать задачу проверки почтовых баз раз в неделю или задачу поиска вирусов в каком-либо каталоге.

Кроме того, вы можете проверить на вирусы любой объект, не создавая для этого специальной задачи проверки. Выбрать объект для проверки можно из интерфейса Антивируса Касперского или стандартными средствами операционной системы Microsoft Windows Server (например, в окне программы **Проводник** или на **Рабочем столе** и т.д.).

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

8.1. Управление задачами поиска вирусов

Запуск задач проверки на вирусы осуществляется вручную или автоматически по сформированному расписанию (см. п. 6.5 на стр. 68).

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.

8.2. 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. 23).

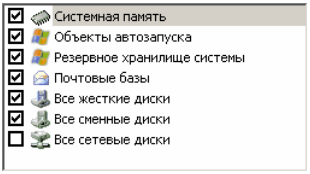


Рисунок 23. Список объектов для проверки

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 Server, например, в окне программы **Проводник** или на **Рабочем столе** и т.д. (см. рис. 24). Для этого установите курсор мыши на имени выбранного объекта, правой клавишей мыши откройте контекстное меню Microsoft Windows Server и выберите пункт **Проверить на вирусы**.

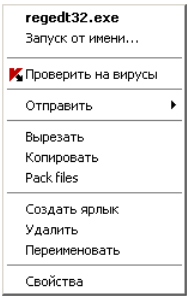


Рисунок 24. Проверка объекта из контекстного меню Microsoft Windows Server

8.3. Создание задач поиска вирусов

Для проверки объектов сервера 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 могут быть созданы. 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. 8.2 на стр. 87), указать параметры, с которыми будет выполняться задача (см. п. 8.4 на стр. 90), а

также, если требуется, настроить расписание (см. п. 6.5 на стр. 68) 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.

8.4. Настройка задач поиска вирусов

То, каким образом осуществляется проверка объектов на сервере, 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. 8.4.1 на стр. 91);
- перейти к подробной настройке уровня:
    - указать параметры, определяющие типы файлов, подвергаемые анализу на вирусы (см. п. 8.4.2 на стр. 92);

- настроить запуск задач от имени другой учетной записи (см. п. 6.4 на стр. 66);
- указать дополнительные параметры проверки (см. п. 8.4.5 на стр. 98);

- восстановить параметры проверки, используемые по умолчанию (см. п. 8.4.3 на стр. 96);
- выбрать действие, которое будет применено приложением при обнаружении зараженного/ возможно зараженного объекта (см. п. 8.4.4 на стр. 96);
- сформировать расписание автоматического запуска задачи (см. п. 6.5 на стр. 68).

Кроме того, вы можете установить единые параметры запуска для всех задач (см. п. 8.4.6 на стр. 100).

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

8.4.1. Выбор уровня безопасности

Каждая задача проверки на вирусы обеспечивает проверку объектов на одном из следующих уровней (см. рис. 25):

Высокий – максимально полная проверка всего компьютера или отдельного его диска, каталога, файла. Данный уровень мы рекомендуем использовать в случае подозрения сервера 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.

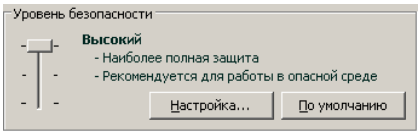


Рисунок 25. Выбор уровня безопасности при проверке объектов на вирусы

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.

8.4.2. 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. 26). 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.

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

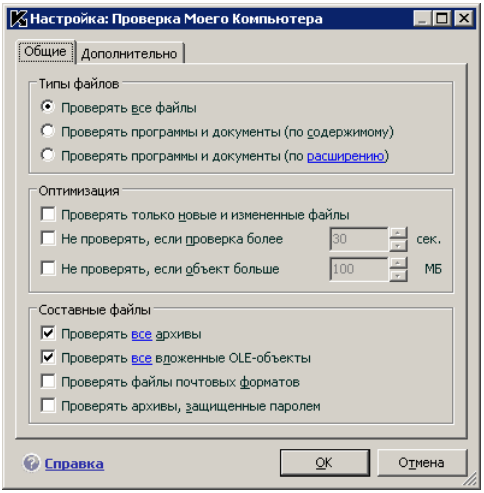


Рисунок 26. Настройка параметров проверки

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.

- **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. 187).

Совет.

Не стоит забывать, что вирус в файле с расширением txt на самом деле 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.

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 при условии, что выбрано действие **Запросить во время проверки/ Запросить по окончании проверки** (см. п. 8.4.4 на стр. 96). 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 Office 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. Если флажок отключен, файлы почтовых форматов будут проверены как бинарные файлы (без разбора формата), и, если файл не заражен, и был выбран параметр Проверять все файлы, в отчет будет занесена информация со статусом *ok*. Если же были выбраны параметры проверки файлов – по типу и расширению, то объект будет пропущен со статусом *исключено по типу*.

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 паролем архивы будут пропущены при проверке.

8.4.3. 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**.

8.4.4. 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. 27).

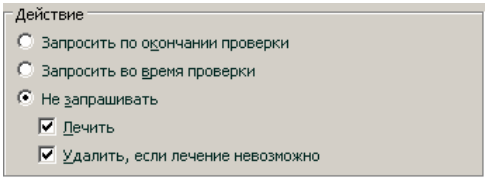


Рисунок 27. Выбор действия над опасным объектом

Если в качестве действия вы выбрали	**При обнаружении вредоносного/ возможно зараженного объекта**
Запросить по окончании проверки	Приложение откладывает обработку объектов до конца проверки. По окончании проверки на экран один за другим будут выводиться окна с запросом действия над каждым из 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 проводя уведомление. Не рекомендуется устанавливать данный режим работы приложения, поскольку зараженные и возможно зараженные объекты остаются на сервере и избежать заражения практически невозможно.
Не запрашивать **Лечить**	Приложение, не запрашивая подтверждения, выполняет попытку лечения обнаруженного объекта. Если объект можно вылечить, то он помещается в резервное хранилище для дальнейшего лечения. Если попытка лечения не удалась, доступ к объекту блокируется.

Если в качестве действия вы выбрали	При обнаружении вредоносного/ возможно зараженного объекта
◉ **Не запрашивать** ☑ **Лечить** ☑ **Удалить, если лечение невозможно**	Приложение, не запрашивая подтверждения, выполняет попытку лечения обнаруженного объекта. Если попытка лечения объекта не удалась, он удаляется. Копия объекта сохранятеся в резервном хранилище.
◉ **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. 11.2 на стр. 124) на тот случай, если понадобится восстановить объект или появится возможность его вылечить.

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

8.4.5. Дополнительные параметры поиска вирусов

Кроме настройки основных параметров проверки на вирусы вы можете установить дополнительные параметры (см. рис. 28):

☑ **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 антивирусные базы, архив будет проверен повторно.

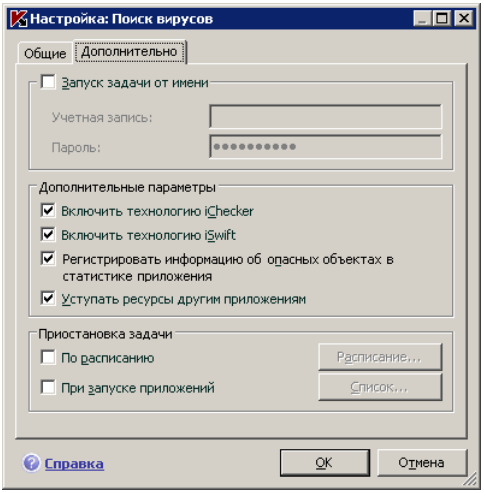


Рисунок 28. Дополнительная настройка проверки

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

Включить технологию iSwift. Данная технология является развитием технологии iChecker для компьютеров с файловой системой NTFS. Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе, а также применима только к объектам, расположенным в файловой системе NTFS.

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. 11.3.2 на стр. 130). 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.

8.4.6. 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. 8.4.1 на стр. 91), произведите дополнительную настройку уровня, укажите действие над объектами (см. п. 8.4.4 на стр. 96).
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 9. ТЕСТИРОВАНИЕ РАБОТЫ АНТИВИРУСА КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS SERVERS

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

9.1. 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.

9.2. 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. 9.1 на стр. 101), 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 (см. п. 11.3.1 на стр. 129).
3. Запустите файл тестового «вируса» или его модификацию на выполнение.

Файловый Антивирус перехватит обращение к файлу, проверит его и удалит.

Выбирая различные варианты предварительных настроек 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.

9.3. 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. 9.1 на стр. 101), а также созданные вами модификации тестового «вируса».
2. Создайте новую задачу поиска вирусов (см. п. 8.3 на стр. 89) и в качестве объекта проверки выберите папку, содержащую набор тестовых «вирусов» (см. п. 9.1 на стр. 101).
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. 8.1 на стр. 87) поиска вирусов на выполнение.

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

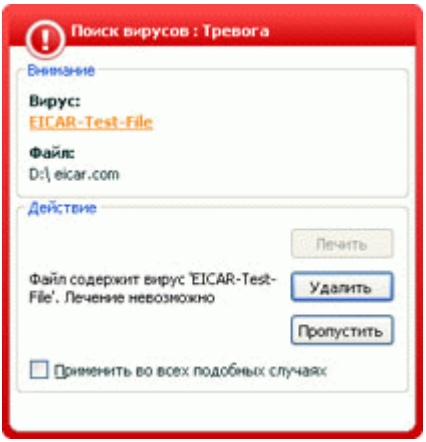


Рисунок 29. Обнаружен опасный объект

Таким образом, выбирая различные варианты предварительных настроек 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 10. ОБНОВЛЕНИЕ ПРИЛОЖЕНИЯ

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

Обновление приложения подразумевает загрузку и установку на сервер:

- **Сигнатур угроз**

  Защита информации на сервере обеспечивается на основании сигнатур угроз. Компоненты защиты используют их при поиске опасных объектов на сервере и их обезвреживании. Сигнатуры ежечасно пополняются записями о новых угрозах и способах борьбы с ними. Поэтому настоятельно рекомендуется регулярно обновлять их.

  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 сервер. 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 приложения 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 сервер 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 сервере сравниваются с расположенными в источнике обновлений. В случае если на сервере установлена последняя версия сигнатур и модулей, в окне приложения это отмечено соответствующей записью. Если сигнатуры и модули отличаются, то на сервер 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. 10.2 на стр. 108) 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. 10.4.4 на стр. 116). Данный сервис позволяет обновлять базы сигнатур угроз и модули, используемые приложениями версии 6.0, на компьютерах сети в целях экономии интернет-трафика.

10.1. Запуск обновления

В любой момент вы можете запустить обновление приложения. Оно будет производиться из выбранного вами источника обновлений (см. п. 10.4.1 на стр. 110).

Запустить обновление приложения вы можете:

- из контекстного меню (см. п. 4.2 на стр. 39);
- из главного окна приложения (см. п. 4.3 на стр. 40).

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. 10.4.4 на стр. 116).

10.2. 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.

10.3. 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. Поэтому вам потребуется провести дополнительную настройку: указать источник обновления (см. п. 10.4.1 на стр. 110), параметры сетевого подключения (см. п. 10.4.3 на стр. 114), а также, если требуется, включить запуск задачи с правами (см. п. 6.4 на стр. 66) и настроить расписание (см. п. 6.5 на стр. 68).

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.

10.4. Настройка обновления

Обновление приложения выполняется в строгом соответствии с параметрами, определяющими:

- с какого ресурса производится копирование и установка обновлений приложения (см. п. 10.4.1 на стр. 110);
- в каком режиме запускается процесс обновления приложения и что именно обновляется (см. п. 10.4.2 на стр. 113);
- как часто требуется запускать обновление, в случае если настроен запуск по расписанию (см. п. 6.5 на стр. 68);
- от имени какой учетной записи будет выполнено обновление (см. п. 6.4 на стр. 66);
- требуется ли копировать полученные обновления в локальный каталог (см. п. 10.4.4 на стр. 116);
- какие действия нужно выполнять после обновления приложения (см. п. 10.4.4 на стр. 116).

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

10.4.1. Выбор источника обновлений

Источник обновлений – это некоторый ресурс, содержащий обновления сигнатур угроз и модулей приложения 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. 30).

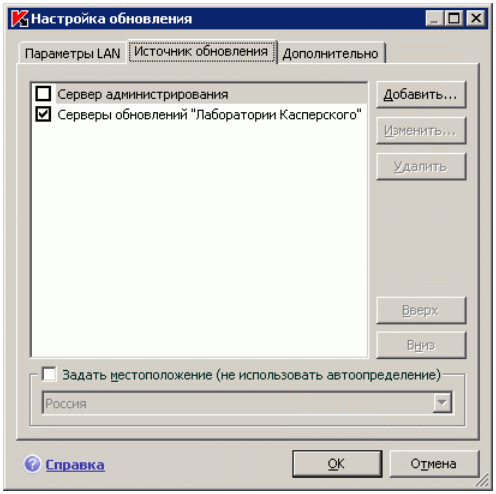


Рисунок 30. Выбор источника обновления

По умолчанию обновление производится с серверов обновлений «Лаборатории Касперского». Список серверов не доступен для редактирования. В процессе обновления Антивирус Касперского обращается к данному списку, выбирает первый по порядку адрес сервера и пытается загрузить с него обновления. Если выполнить обновление с выбранного адреса невозможно, приложение обращается к следующему по списку серверу и вновь пытается получить обновления.

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>.

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» и Kaspersky Administration Kit – это источники, недоступные 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.

10.4.2. Выбор режима и предмета обновления

Важным моментом в настройке обновления приложения является определение предмета обновления и режима обновления.

Предмет обновления (см. рис. 31) определяет, что именно будет обновляться:

- сигнатуры угроз;
- модули приложения.

Сигнатуры угроз обновляются всегда, а модули приложения – только в том случае, если установлен соответствующий режим.

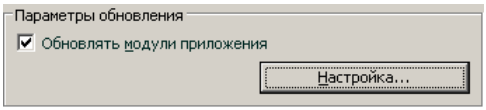


Рисунок 31. Выбор предмета обновления

Чтобы в процессе обновления на сервер 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. 32) 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 (см. п. 10.4.1 на стр. 110). При обнаружении свежих обновлений Антивирус скачивает их и устанавливает на компьютер.

Если в качестве источника выбран сетевой ресурс, Антивирус Касперского будет производить попытку обновления через интервал, ука-

занный 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 сервер.

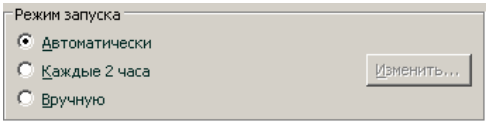


Рисунок 32. Выбор режима запуска обновления

- **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. 68). Такой режим обновления используется по умолчанию.
- **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 (если включен сервис уведомлений) соответствующего содержания (см. п. 11.8.1 на стр. 141);
  - во-вторых, второй индикатор на главном окне приложения сообщит о том, что защита на вашем компьютере устарела (см. п. 5.1.1 на стр. 44);
  - в-третьих, в разделе комментариев и советов главного окна появится рекомендация по обновлению приложения (см. п. 4.3 на стр. 40).

10.4.3. 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. 33).

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.

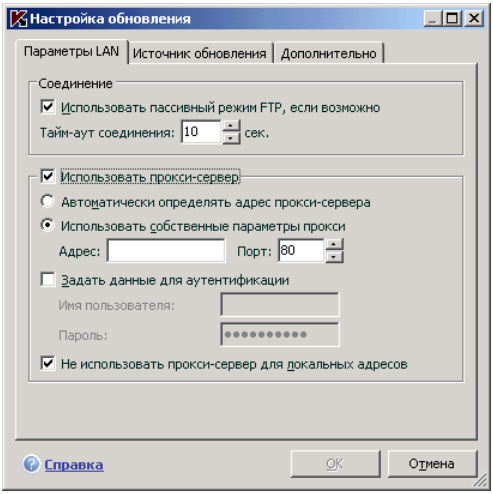


Рисунок 33. Настройка сетевых параметров обновления

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.

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. 66).

  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**.

10.4.4. 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. 34) установите флажок **Копировать в папку** и в поле ниже укажите путь к папке общего доступа, куда будут помещаться полу-

ченные 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.

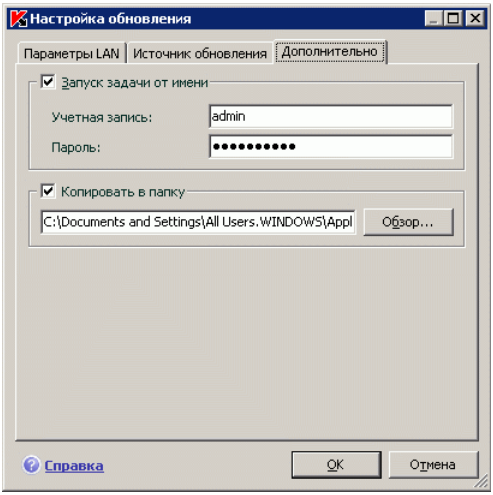


Рисунок 34. Настройка сервиса копирования обновлений

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.

10.4.5. Действия после обновления приложения

Каждое обновление сигнатур угроз содержит в себе новые записи, позволяющие защищать сервер 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. 11.1 на стр. 120). 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 сервера. 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 8 на стр. 86). Рекомендуем настроить автоматический режим запуска данной задачи после каждого обновления сигнатур угроз (см. п. 6.5 на стр. 68).

ГЛАВА 11. 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. 11.2 на стр. 124). 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. 11.1 на стр. 120).

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. 11.6 на стр. 137). 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. 11.8.1 на стр. 141). 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 администраторов сервера на выполнение некоторых действий с Антивирусом Касперского (см. п. 11.8.2 на стр. 143). На-

пример, изменение уровня защиты может значительно повлиять на безопасность информации на сервере.

- 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. 11.5 на стр. 135).

Также приложение предоставляет детальную справочную информацию (см. п. 11.4 на стр. 134) и подробные отчеты (см. п. 11.3 на стр. 126) о работе Файлового Антивируса и выполнении всех задач поиска вирусов, обновления.

Вам также предоставляется возможность изменять внешний вид Антивируса Касперского и настраивать параметры текущего интерфейса приложения (см. п. 11.7 на стр. 138).

Рассмотрим подробнее все перечисленные сервисы.

11.1. Карантин возможно зараженных объектов

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

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

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

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

  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 измененной вредоносной программой, к возможно зараженным объектам и обязательно укажет, на какую угрозу похоже это заражение.

- Код обнаруженного объекта напоминает по структуре вредоносную программу, однако в 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.

Вы сами можете поместить объект на карантин, нажав на кнопку **Карантин** в специальном уведомлении, которое открывается на экране сервера 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.

11.1.1. 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. 35) 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.

- 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.

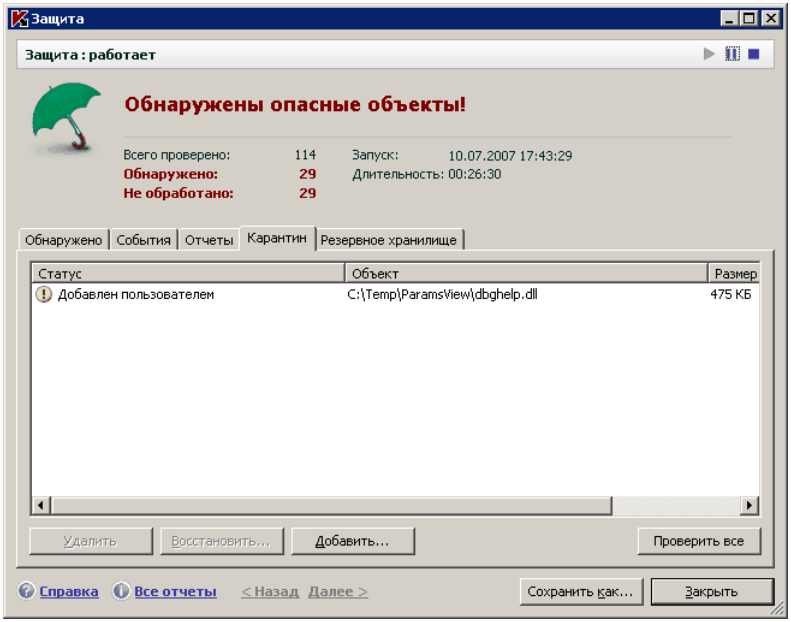


Рисунок 35. Список объектов на карантине

- Восстанавливать файлы в заданный каталог 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 сервера!

- 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**.

11.1.2. 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. 10.4.4 на стр. 116).

  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. 36) укажите временной период, после которого объекты, находящиеся в хранилище, будут автоматически удалены.

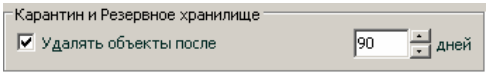


Рисунок 36. Настройка срока хранения объектов на карантине

11.2. 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.

11.2.1. 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. 37) 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.

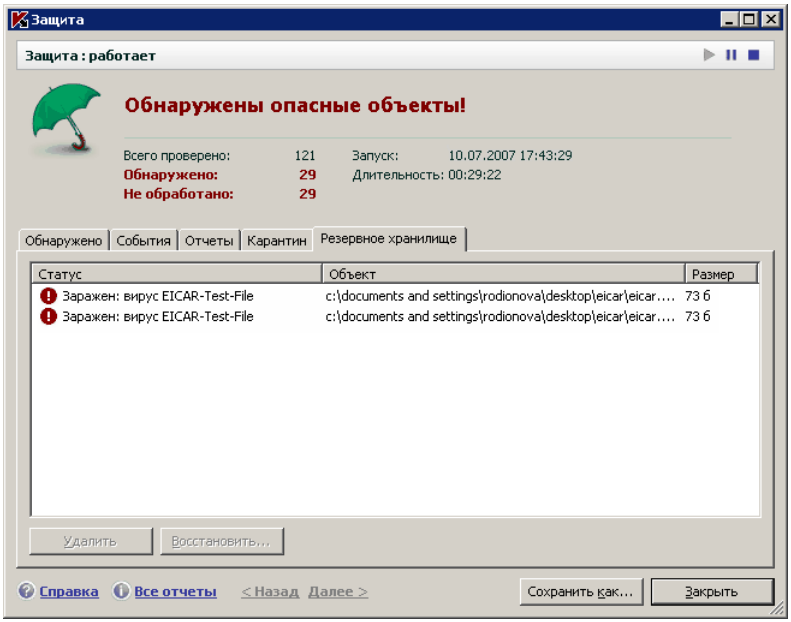


Рисунок 37. Резервные копии удаленных или вылеченных объектов

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 сервера.

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. 11.2.2 на стр. 126).

11.2.2. Настройка параметров резервного хранилища

Вы можете определить максимальный срок хранения копий в резервном хранилище.

По умолчанию срок хранения копий опасных объектов составляет 90 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. 36) правой части окна.

11.3. Отчеты

Работа *Файлового Антивируса* приложения Антивирус 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. 38). Здесь приведены последние отчеты по Файловому Антивирусу, задачам поиска вирусов и обновления, запущенным в текущей сессии работы Антивируса Касперского. Напротив Файлового Антивируса или задачи указан результат работы. Например, *прервано* или *завершено*. Если вы хотите просмотреть полную историю формирования отчетов текущей сессии работы приложения, установите флажок ☑ **Показывать историю отчетов**.

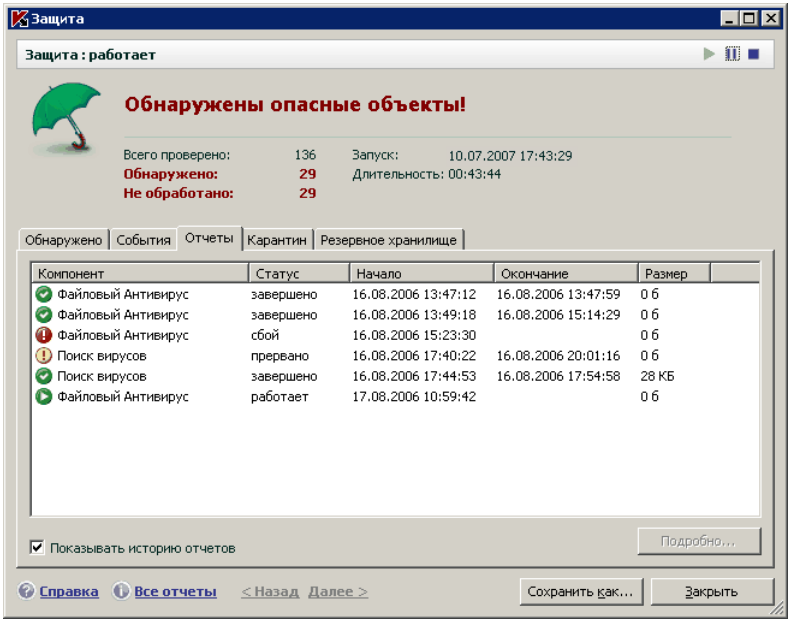


Рисунок 38. Отчеты о работе компонентов приложения

Чтобы ознакомиться со всеми событиями, зафиксированными в отчете о работе Файлового Антивируса или выполнении задачи,

выберите Файловый Антивирус или задачу на закладке **Отчеты** и нажмите на кнопку **Подробно**.

В результате будет открыто окно, содержащее детальную информацию о работе Файлового Антивируса или задачи. Результирующая статистика работы приведена в верхней части окна, а подробная информация размещена на разных закладках в центральной части:

- Закладка **Обнаружено** содержит список опасных объектов, обнаруженных в результате работы Файлового Антивируса или выполненной задачи поиска вирусов.
- Закладка **События** отражает все события в работе Файлового Антивируса или задачи.
- Закладка **Статистика** включает подробную статистику всех проверенных объектов.
- Закладка **Параметры** отображает набор параметров, в соответствии с которыми работает Файловый Антивирус, задача поиска вирусов или обновление сигнатур угроз.

- Закладка **Заблокированные пользователи** отображает список пользователей, компьютеры которых были заблокированы при попытке произвести копирование зараженного или возможно зараженного объекта на сервер.

Весь отчет вы можете импортировать в текстовый файл. Например, это полезно в том случае, если в работе Файлового Антивируса 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 просматриваете, список пунктов меню отличается, ниже приведены все возможные пункты):

Лечить – произвести попытку лечения опасного объекта. Если обезвредить объект не получится, вы можете оставить его в этом списке для отложенной проверки с обновленными 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.

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.

11.3.1. Настройка параметров отчетов

Для настройки параметров формирования и хранения отчетов:

Откройте окно настройки Антивируса Касперского по ссылке Настройка из главного окна приложения.

1. Выберите **Файлы данных** в дереве настройки.
2. В блоке **Отчеты** (см. рис. 39) 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 90 дней, по истечении которого отчеты удаляются. Вы можете изменить максимальный срок хранения или отменить такое ограничение вообще.

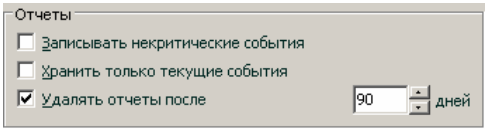


Рисунок 39. Настройка параметров формирования отчетов

11.3.2. Закладка *Обнаружено*

Данная закладка (см. рис. 40) 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**.

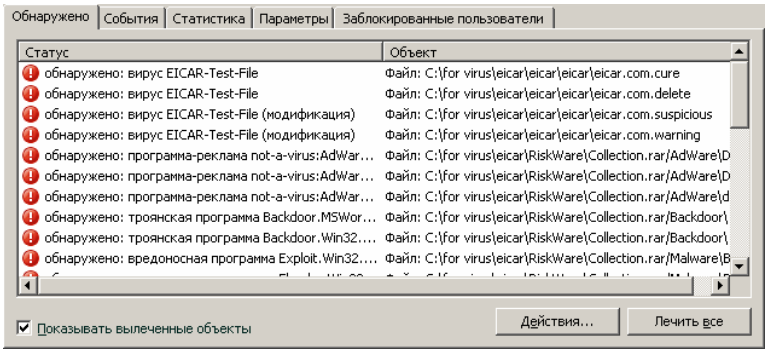


Рисунок 40. Список обнаруженных опасных объектов

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.

11.3.3. Закладка *События*

Полный список всех важных событий в работе Файлового Антивируса или при выполнении задачи поиска вирусов либо обновления сигнатур угроз фиксируется на данной закладке (см. рис. 41).

События могут быть следующих типов:

Критические события – события критической важности, указывающие на проблемы в работе приложения или на уязвимости в защите сервера. 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**.

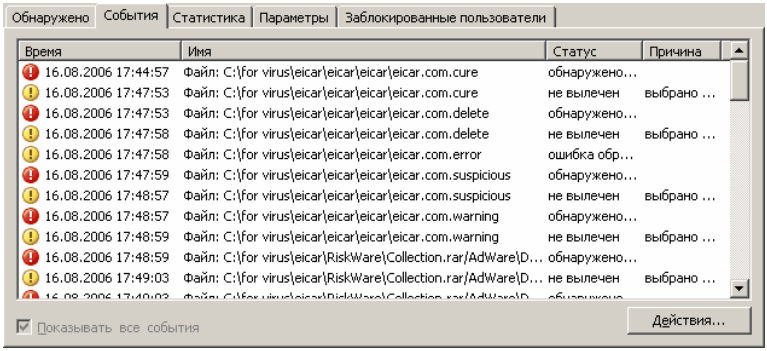


Рисунок 41. События, возникшие в работе компонента

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.

11.3.4. Закладка *Статистика*

Подробная статистика работы Файлового Антивируса или выполнения задачи поиска вирусов фиксируется на данной закладке (см. рис. 42). Здесь вы можете узнать:

- Сколько объектов было проверено на наличие опасных объектов в текущем сеансе работы Файлового Антивируса 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.

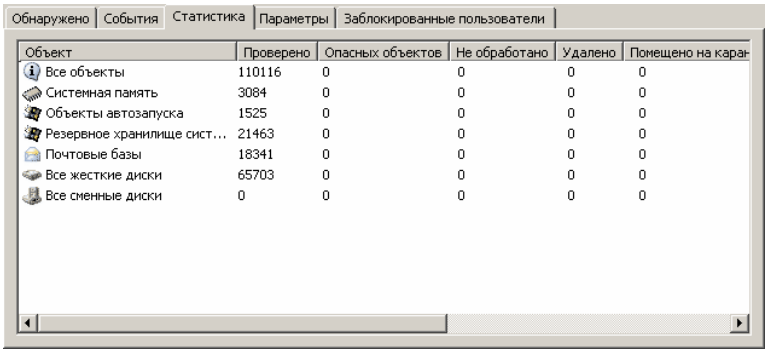


Рисунок 42. Статистика работы компонента

11.3.5. Закладка *Параметры*

Полный обзор параметров, в соответствии с которым работает Файловый Антивирус, выполняется задача поиска вирусов или обновление приложения, приводится на закладке **Параметры** (см. рис. 43). Вы можете узнать, какой уровень защиты обеспечивает работа Файлового Антивируса, 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 приложения** установлен. При этом приложение отслеживает уровень загрузки процессора и дисковых подсистем на предмет актив-

ности 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.

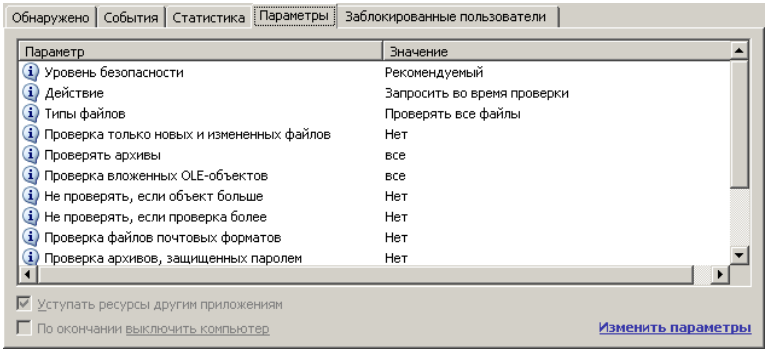


Рисунок 43. Параметры работы компонента

- Установить режим работы компьютера после завершения задачи проверки на вирусы. Вы можете настроить выключение / перезагрузку сервера либо переход в режим ожидания или спящий режим. Для выбора варианта щелкайте левой клавишей мыши по гиперссылке пока она не примет нужное значение.

11.3.6. Закладка *Заблокированные пользователи*

Список пользователей, у которых временно заблокирован доступ к серверу, представлен на закладке **Заблокированные пользователи** (см. рис. 44). Блокировка применяется для каждого компьютера, с которого была произведена попытка копирования на сервер зараженного или возможно зараженного объекта. Блокирование компьютера может быть применено дополнительно к действиям, связанным с обработкой этого объекта – лечению или удалению.

На закладке вы можете узнать, какие компьютеры были заблокированы, а также, дату и время, когда это произошло, и сколько часов осталось до их разблокировки.

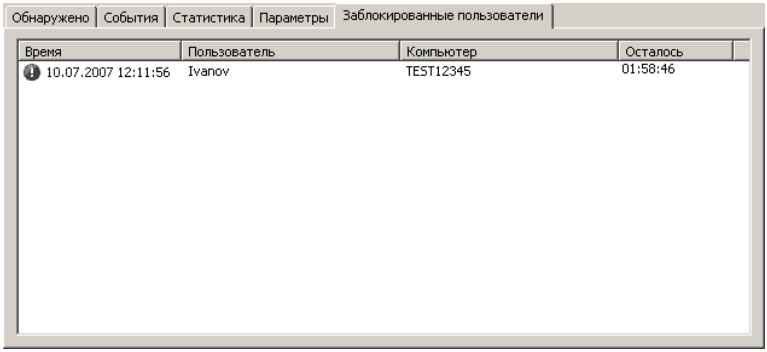


Рисунок 44. Список заблокированных пользователей

11.4. Общая информация о приложении

Общую информацию о приложении вы можете просмотреть в разделе **Сервис** главного окна (см. рис. 45).

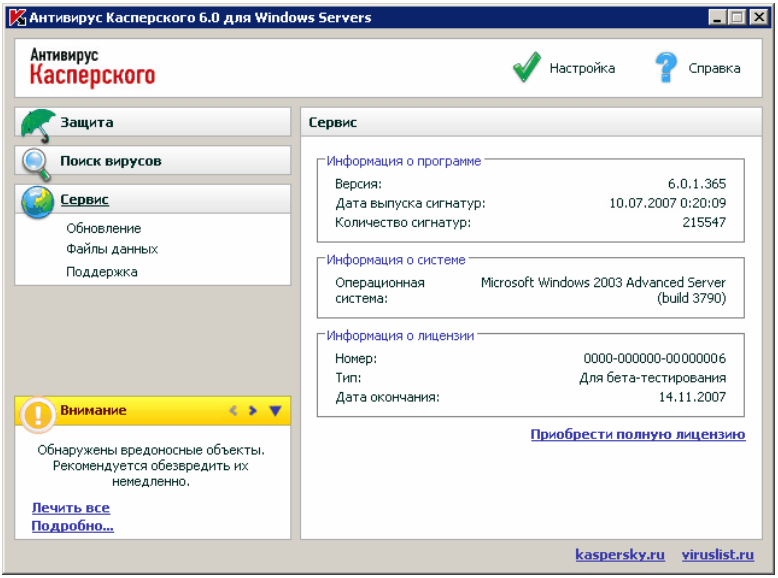


Рисунок 45. Информация о приложении, его лицензии и системе, на которую оно установлено

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 сервере 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. 11.6 на стр. 137).

11.5. 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 производится 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 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 сервера 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. 46). 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.

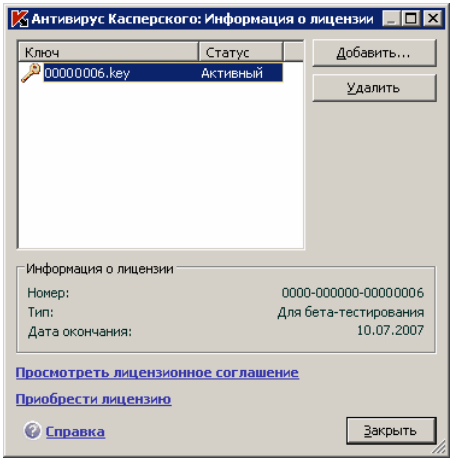


Рисунок 46. Информация о лицензии

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 программы. Для перехода в окно управления лицензиями щелкните левой клавишей мыши в любом месте блока. В открывшемся окне (см. рис. 46) 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. 11.5 на стр. 135). 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 Пиобрести лицензию.

11.6. Техническая поддержка пользователей

Антивирус Касперского предоставляет вам широкие возможности решения вопросов и проблем, связанных с работой приложения. Все они размещены в **Поддержке** (см. рис. 47) раздела **Сервис**.

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 отзыв о приложении или отыскать 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. Попробуйте найти ответ на ваш вопрос или решение вашей проблемы на этом ресурсе.

Чтобы получить техническую поддержку онлайн, воспользуйтесь ссылкой База знаний.

Отзывы о работе программы. 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 конфигу-

рацию системы или воспользоваться автоматическим сбором информации о вашем компьютере.

Чтобы перейти к форме отзывов, воспользуйтесь ссылкой Сообщите об ошибке или оставьте отзыв о приложении.

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.

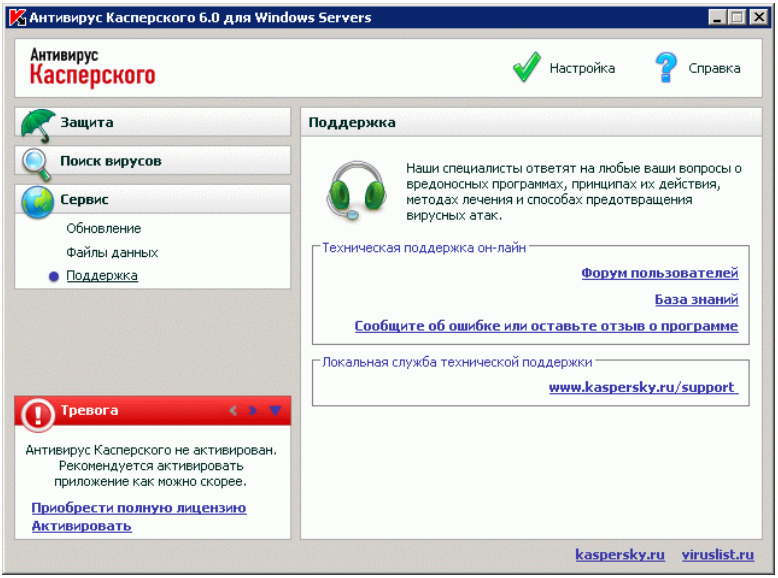


Рисунок 47. Информация о технической поддержке

11.7. 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. 48).

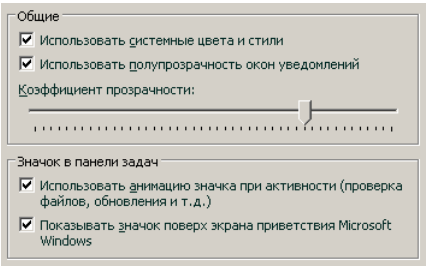


Рисунок 48. Настройка параметров интерфейса приложения

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 сервера от любого рода угроз включена. Если вы не хотите использовать индикатор защиты, снимите флажок **Показывать значок поверх экрана приветствия Microsoft Windows**.

- Использовать или нет анимацию значка приложения в системной панели.

  В зависимости от выполняемой приложением операции значок в системной панели меняется. 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 сервера: 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 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**.

- 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 **Папка 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.

11.8. 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.

11.8.1. 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. 49).

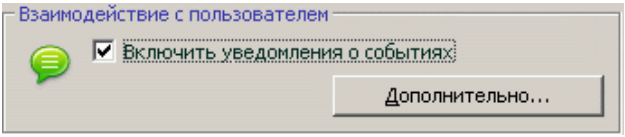


Рисунок 49. Включение режима уведомлений

2. Определить типы событий Антивируса Касперского, о возникновении которых вы хотите быть уведомлены, и способ уведомлений (см. п. 11.8.1.1 на стр. 142).
3. Настроить параметры отправки уведомлений по электронной почте, если предполагается именно такой способ уведомлений (см. п. 11.8.1.2 на стр. 143).

11.8.1.1. 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 сервера. 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. 50) вы можете настроить следующие способы уведомлений о перечисленных выше событиях:

- *Всплывающее сообщение* над значком приложения в системной панели, содержащее информационное сообщение о возникшем событии.

  Чтобы использовать данный тип уведомления, установите флажок в графе **Экран** напротив события, о котором вы хотите быть уведомлены.

- *Звуковое оповещение*.

  Если вы хотите, чтобы данное уведомление сопровождалось звуковым сигналом, установите в графе **Звук** флажок напротив события.

- *Уведомление по электронной почте*.

  Чтобы использовать данный тип уведомления, установите флажок в графе **E-mail** напротив события, о котором вы хотите быть уведомлены, и настройте параметры отправки уведомлений (см. п. 11.8.1.2 на стр. 143).

- *Запись информации в журнал событий*.

  Чтобы фиксировать информацию о наступлении какого-либо события в журнале, установите напротив него флажок в графе **Журнал** и настройте параметры журнала событий (см. п. 11.8.1.3 на стр. 144).

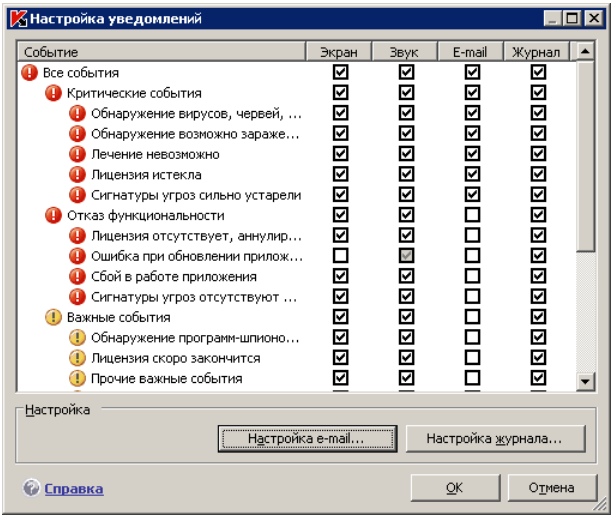


Рисунок 50. События в работе приложения и способы уведомлений о них

11.8.1.2. Настройка отправки уведомлений по электронной почте

После того как вы выбрали события (см. п. 11.8.1.1 на стр. 142), 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** 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**.

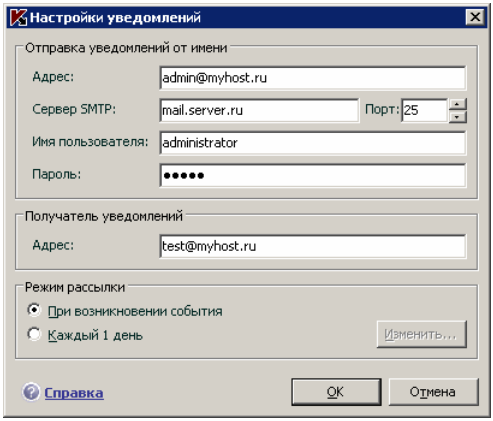


Рисунок 51. Настройка параметров уведомления по электронной почте

   - 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.

11.8.1.3. 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**).

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

11.8.2. Самозащита приложения и ограничение доступа к нему

Антивирус Касперского является приложением, обеспечивающим безопасность сервера 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, сервер может использоваться несколькими администраторами, в том числе с разным уровнем компьютерной грамотности. Открытый доступ к приложению, его параметрам может значительно снизить уровень безопасности сервера в целом.

Чтобы обеспечить стабильность системы безопасности сервера, в приложение добавлены механизмы самозащиты, защиты от удаленного воздействия, а также защита доступа к приложению паролем.

Чтобы включить использование механизмов самозащиты приложения:

1. Откройте окно настройки приложения по ссылке Настройка главного окна.

2. Выберите пункт **Сервис** в дереве настройки.

В блоке **Самозащита** (см. рис. 52) 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 отлючен пользователем).

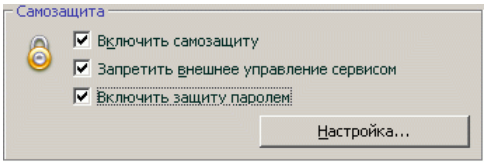


Рисунок 52. Настройка защиты приложения

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. 53).

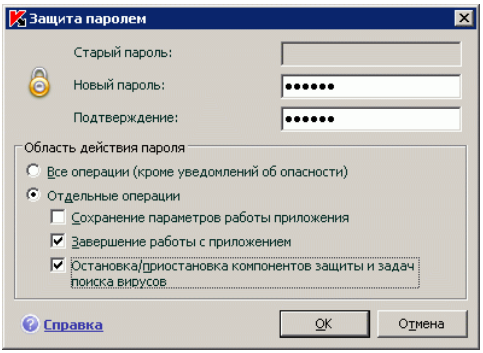


Рисунок 53. Настройка защиты приложения паролем

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 сервера или приостановить ее на некоторое время.

Каждое из перечисленных выше действий приводит к снижению уровня защиты сервера, поэтому необходимо определить круг людей, которые будут работать с сервером.

Теперь при попытке пользователя выполнить на сервере выбранные вами действия приложение всегда будет запрашивать пароль.

11.8.3. 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.

11.9. Экспорт / импорт параметров работы Антивируса Касперского

Антивирус Касперского предоставляет вам возможность экспорта и импорта своих параметров.

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.

11.10. 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.

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. 28). Следуйте его указаниям.

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

ГЛАВА 12. 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 Servers 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 Servers 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»);
- на файловых серверах сети разверните Антивирус Касперского 6.0 для Windows Servers и *Агент администрирования* (входящий в состав Kaspersky Administration Kit). Подробнее об удаленной установке Антивируса Касперского на компьютеры сети смотрите Руководство по внедрению «Kaspersky Administration Kit».

Перед обновлением версии плагина управления Антивирусом Касперского через Kaspersky Administration Kit завершите работу Консоли администрирования.

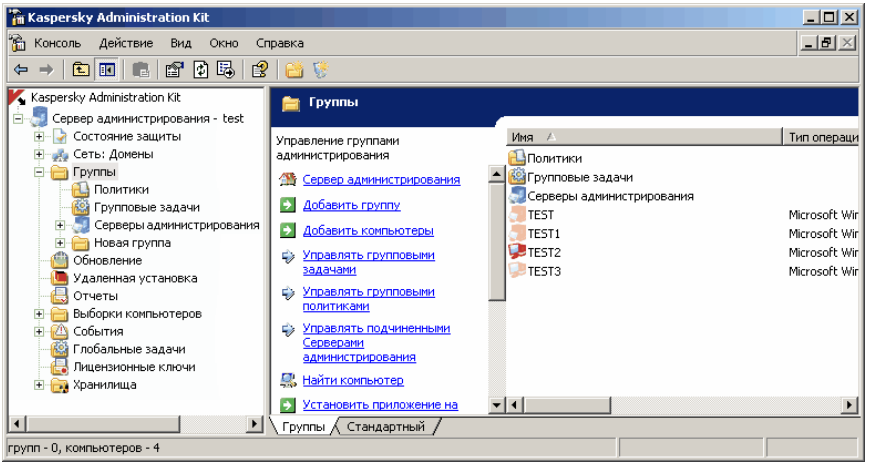


Рисунок 54. Консоль администрирования Kaspersky Administration Kit

Доступ к управлению приложением через Kaspersky Administration Kit обеспечивает *Консоль администрирования* (см. рис. 54). Она представляет собой стандартный **интерфейс, интегрированный в MMC** (Microsoft Management Console), и позволяет администратору выполнять следующие функции:

- удаленно устанавливать Антивирус Касперского 6.0 для Windows Servers и *Агент администрирования* на компьютеры сети;
- удаленно настраивать Антивирус Касперского на компьютерах сети;
- обновлять сигнатуры угроз и модули Антивируса Касперского;
- осуществлять управление лицензиями для приложения 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 для приложения Антивирус Касперского для Windows Servers разделяют по типам (задача поиска вирусов, задача обновления приложения, отката обновлений, задача установки лицензионного клю-

ча). Каждой конкретной задаче соответствует набор параметров работы Антивируса Касперского при ее выполнении – *параметры задачи*.

Особенностью централизованного управления является организация удаленных компьютеров в группы и управление их настройками 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.

12.1. Управление приложением

Kaspersky Administration Kit предоставляет возможность удаленного управления запуском и остановкой Антивируса Касперского на отдельном клиентском компьютере, а также настройки общих параметров работы приложения, таких как включение / отключение защиты компьютера, настройка параметров резервного и карантинного хранилищ, а также настройка параметров формирования отчетов.

Для управления параметрами приложения:

1. В папке **Группы** (см. рис. 54) выберите папку с названием группы, в состав которой входит клиентский компьютер.
2. В панели результатов выберите компьютер, для которого вам необходимо изменить параметры приложения. В контекстном меню или в меню **Действия** выберите команду **Свойства**.
3. В окне свойств клиентского компьютера на закладке **Приложения** (см. рис. 55) представлен полный список приложений «Лаборатории Касперского», установленных на клиентском компьютере. Выберите приложение **Антивирус Касперского 6.0 для Windows Servers**.

Под списком приложений расположены кнопки управления, с помощью которых вы можете:

1. просмотреть список событий в работе приложения, произошедших на клиентском компьютере и зарегистрированных на Сервере администрирования;
2. просмотреть текущую статистическую информацию о работе приложения;

3. произвести настройку параметров приложения (см. п. 12.1.2 на стр. 153).

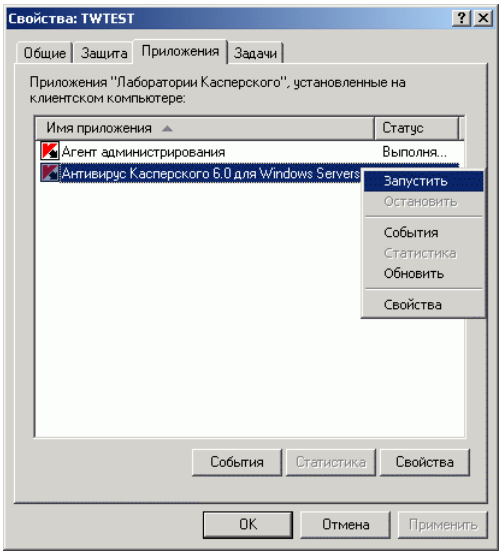


Рисунок 55. Список приложений «Лаборатории Касперского»

12.1.1. Запуск / остановка приложения

Управление запуском / остановкой Антивируса Касперского на удаленном компьютере осуществляется с помощью команд контекстного меню в окне свойств компьютера (см. рис. 55).

Аналогичные действия можно выполнить с помощью кнопок **Запустить / Остановить** из окна настройки параметров приложения на закладке **Общие** (см. рис. 56).

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.

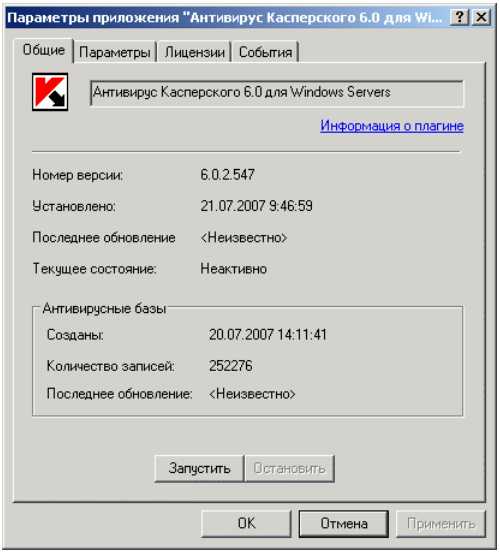


Рисунок 56. Настройка параметров Антивируса Касперского. Закладка **Общие**

12.1.2. Настройка параметров приложения

Для того чтобы просмотреть или изменить параметры работы приложения:

1. Откройте окно свойств клиентского компьютера на закладке **Приложения** (см. рис. 54).
2. Выберите приложение **Антивирус Касперского 6.0 для Windows Servers**. Нажмите на кнопку **Свойства**, чтобы перейти в окно настройки параметров приложения.

Все закладки (кроме закладки **Параметры**) являются стандартными для приложения Kaspersky Administration Kit. Подробное описание стандартных закладок смотрите в одноименном Руководстве администратора.

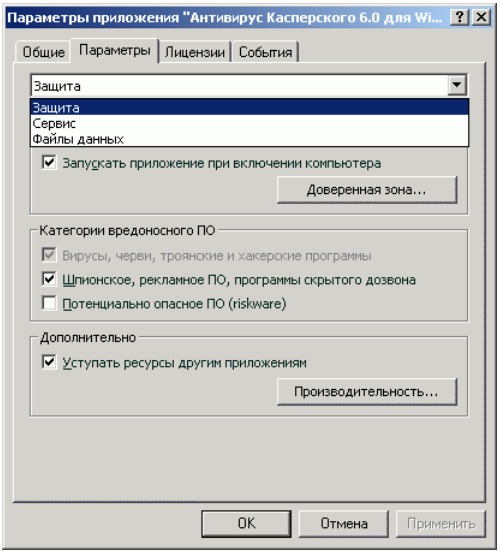


Рисунок 57. Настройка параметров Антивируса Касперского. Закладка **Параметры**

Если для приложения создана политика (см. п. 12.3.1 на стр. 163), 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. 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. 54); • настраивать автоматический запуск приложения при включении компьютера (см. п. 6.1.5 на стр. 58); • формировать доверенную зону и список исключений (см. п. 6.3 на стр. 60); • выбирать виды вредоносных программ, которые будут контролиро-

ваться приложением (см. п. 6.2 на стр. 59);

- настраивать параметры производительности приложения и параметры многопроцессорной конфигурации (см. п. 6.7 на стр. 70).

Сервис

Настройка сервисных параметров включает в себя:

- настройку сервиса получения уведомлений о происходящих событиях (см. п. 11.8.1 на стр. 141);
- управление сервисом самозащиты приложения, ограничивать доступ к настройкам приложения с помощью пароля (см. п. 11.8.2 на стр. 145);
- настройку внешнего вида приложения (см. п. 12.3.1 на стр. 163);
- настройку парметров совместимости Антивируса Касперского с другими приложениями (см. п. 11.8.3 на стр. 147).

Файлы данных

В данном окне вам предлагается настроить параметры формирования отчетной статистики по работе приложения (см. п. 11.3.1 на стр. 129), а также указать время хранения файлов в резервном хранилище (см. п. 11.2.2 на стр. 126) и на карантине (см. п. 11.1.2 на стр. 123).

12.1.3. 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. 55).
2. Выберите приложение **Антивирус Касперского 6.0 для Windows Servers** и воспользуйтесь кнопкой **Свойства**. В результате будет открыто окно настройки параметров приложения (см. рис. 57). 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 компьюте-

ре: 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. 47).

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**.

Вы можете редактировать список ссылок 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.

12.2. Управление задачами

В данном разделе приведена информация об управлении задачами для Антивируса Касперского 6.0 для Windows Servers. Подробнее о концепции управления задачами через Kaspersky Administration Kit 6.0 смотрите Руководство администратора по данному продукту.

При установке приложения для каждого компьютера будет сформирован набор системных задач. В этот список (см. рис. 58) входят задачи защиты (Файловый Антивирус), задачи поиска вирусов (Проверка Моего Компьютера, Проверка объектов автозапуска, Проверка критических областей) и задачи обновления (обновление сигнатур угроз и модулей приложения, откат обновления).

Вы можете запускать системные задачи, настраивать их параметры и расписание; удаление данных задач невозможно.

Кроме того, вы можете создавать собственные задачи, например, задачи поиска вирусов, обновления приложения и отката обновления, задача установки лицензионного ключа.

Для того чтобы просмотреть список задач, сформированных для клиентского компьютера:

1. В папке **Группы** (см. рис. 54) 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 **Действия**. В результате в главном окне приложения откроется окно просмотра свойств клиентского компьютера.
3. На закладке **Задачи** (см. рис. 58) представлен полный список задач, сформированных для данного клиентского компьютера.

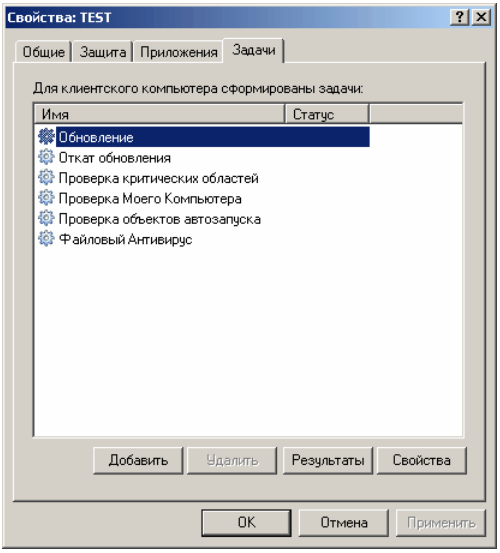


Рисунок 58. Список задач приложения

12.2.1. Запуск и остановка задач

Запуск задач на клиентском компьютере выполняется только в том случае, если запущено соответствующее приложение (см. п. 12.1.1 на стр. 152). При остановке приложения выполнение всех запущенных задач прекращается.

Запуск и остановка задач осуществляется автоматически (в соответствии с расписанием), а также вручную (при помощи команд контекстного меню), а также из окна просмотра настроек задачи. Вы можете также приостановить процесс выполнения запущенной задачи и потом 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. 59) при помощи одноименных кнопок.

12.2.2. Создание задач

При работе с приложением через Kaspersky Administration Kit вы можете создавать:

- локальные задачи – определяются для отдельного компьютера;
- групповые задачи – определяются для компьютеров, объединенных в одну логическую группу;
- глобальные задачи – определяются для произвольного набора компьютеров из произвольных групп логической сети.

Вы можете вносить изменения в настройки 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**.

12.2.2.1. Создание локальной задачи

Для создания локальной задачи выполните следующие действия:

1. Откройте окно свойств клиентского компьютера на закладке **Задачи** (см. рис. 58).
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 пре-

кращения 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 Servers. А также 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 ключ*а – 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 сформировать список объектов проверки (см. п. 8.2 на стр. 87) и указать действие, которое будет выполнять Антивирус Касперского при обнаружении опасного объекта (см. п. 8.4.4 на стр. 96).

ОБНОВЛЕНИЕ

Для задачи обновления сигнатур угроз и модулей приложения требуется указать источник, из которого будут загружены обновления (см. п. 10.4.1 на стр. 110). 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 (см. п. 6.4 на стр. 66).

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.

12.2.2.2. Создание групповой задачи

Для создания групповой задачи выполните следующие действия:

1. В дереве консоли выберите группу, для которой вы будете создавать задачу.
2. Выберите входящую в ее состав папку **Групповые задачи**, вызовите контекстное меню и выберите команду **Создать → Задачу**, или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер создания задачи, аналогичный масте-

ру создания локальной задачи (подробнее см. п. 12.2.2.1 на стр. 158). 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.

12.2.2.3. Создание глобальной задачи

Для создания глобальной задачи выполните следующие действия:

1. Выберите в дереве консоли узел **Глобальные задачи**, 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. 12.2.2.1 на стр. 158). Исключением является 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»).

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.

12.2.3. Настройка параметров задач

Для просмотра и изменения параметров задач клиентского компьютера:

1. Откройте окно свойств клиентского компьютера на закладке **Задачи** (см. рис. 58).
2. Выберите задачу в списке и нажмите на кнопку **Свойства**. В результате будет открыто окно настройки параметров задачи (см. рис. 60).

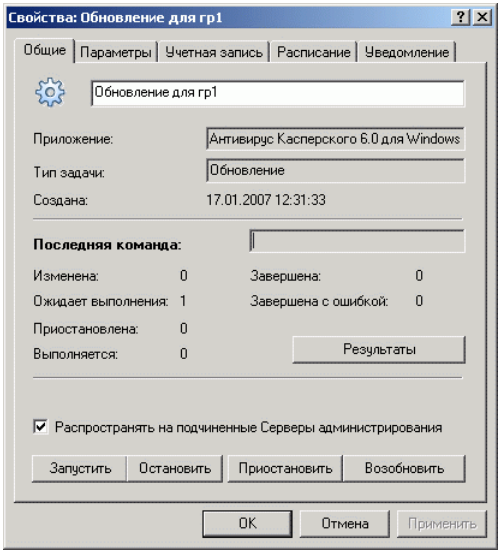


Рисунок 59. Настройка параметров задачи

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 являются специфическими для данной задачи. Подробное описание настройки параметров задач смотрите в разделах Глава 7 – Глава 10 на стр. 72 – 106 текущей документации.

Если для приложения создана политика (см. п. 12.3 на стр. 162), в которой запрещено переопределение некоторых параметров, то их изменение при настройке задач будет недоступно.

12.3. 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 Servers. Подробнее о концепции управления политиками через Kaspersky Administration Kit 6.0 смотрите Руководство администратора по данному продукту.

12.3.1. Создание политики

Чтобы создать политику для Антивируса Касперского, выполните следующие действия:

1. В папке **Группы** (см. рис. 54) выберите группу компьютеров, для которой нужно создать политику.
2. Выберите входящую в состав выбранной группы папку **Политики**, откройте контекстное меню и воспользуйтесь командой **Создать → Политику**. На экране появится окно создания новой политики.

   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**.

На каждом шаге создания политики, введенные параметры можно зафиксировать с помощью кнопки  . Если замок на кнопке закрыт, то в дальнейшем при использовании политики на клиентских компьютерах будут использоваться значения, заданные создаваемой политикой.

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 Servers** из раскрывающегося списка **Имя приложения**. Для того чтобы настройки политики вступили в силу сразу после ее создания, следует установить флажок **Сделать политику активной**.

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 включить/ отключить защиту компьютера, а также Файловый Антивирус. По умолчанию защита включена и Файловый Антивирус работает.

Чтобы перейти к детальной настройке параметров защиты или настройке Файлового Антивируса, 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. 7.1 на стр. 73). 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. 8.4.4 на стр. 96).

Шаг 5. Настройка параметров обновления

В данном окне вам предлагается настроить параметры обновления Антивируса Касперского.

В блоке **Параметры обновления** укажите, требуется ли выполнять обновление модулей приложения (см. п. 10.4.2 на стр. 113). В окне, открывающемся по кнопке **Настройка**, задайте параметры локальной сети (см. п. 10.4.3 на стр. 114) и укажите источник обновления (см. п. 10.4.1 на стр. 110).

В блоке **Действия после обновления** включите / отключите проверку карантинного хранилища после получения нового пакета обновлений (см. п. 10.4.4 на стр. 116).

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 Антивируса Касперского будет добавлена в папку **Политики** 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, переносить политики из одной группы в другую и удалять при помощи стандартных команд контекстного меню **Копировать** / **Вставить**, **Вырезать** / **Вставить** и **Удалить** или аналогичных пунктов в меню **Действие**.

12.3.2. 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. Выберите группу компьютеров в дереве консоли в папке **Группы**, для которой необходимо отредактировать настройки.
2. Выберите входящую в состав данной группы папку **Политики**, при этом в панели результатов будут отображены все политики, созданные для группы.
3. Выберите в списке политик нужную политику для **Антивируса Касперского 6.0 для Windows Servers** (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. 60).

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. 12.1.2 на стр. 153) и параметры задач (см. п. 12.2 на стр. 156).

Дла настройки параметров из раскрывающегося списка в верхней части окна выберите нужное значение и произведите настройку.

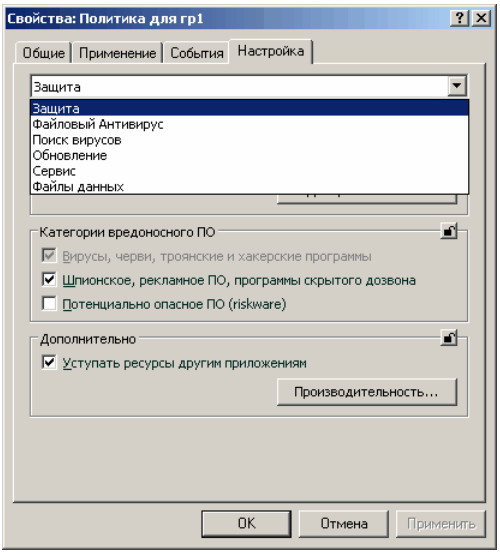


Рисунок 60. Настройка параметров политики

ГЛАВА 13. 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 Файлового Антивируса;
- запуск, остановка, приостановка и возобновления выполнения задач проверки на вирусы;
- получение информации о текущем статусе Файлового Антивируса 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	активации 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 Файлового Антивируса или задачи

PAUSE	приостановка работы Файлового Антивируса или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
RESUME	возобновление работы Файлового Антивируса или задачи
STOP	остановка работы Файлового Антивируса или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
STATUS	вывод на экран текущего статуса Файлового Антивируса или задачи
STATISTICS	вывод на экран статистики по работе Файлового Антивируса или задачи
HELP	помощь по синтаксису команды, вывод списка команд
SCAN	проверка объектов на присутсвие 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.

13.1. 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 параметра:

<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>
```

13.2. Управление Файловым Антивирусом 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 Антивирусу 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 Файловый Антивирус, если он был приостановлен на время кнопкой ❚❚ графического интерфейса или командой `PAUSE` командной строки. В случае если компонент был отключен кнопкой ■ графического интерфейса либо командой `STOP` командной строки, для его запуска необходимо выполнить команду `avp.com START FM`.
FM	Файловый Антивирус
UPDATER	Обновление
RetranslationCfg	Копирование обновлений приложения в локальный источник
Rollback	Откат последнего обновления приложения
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 остановки задачи Мой Компьютер в командной строке введите:

```
avp.com STOP SCAN_MY_COMPUTER /password=<ваш_пароль>
```

13.3. 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. 13.2 на стр. 169). 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 при обнаружении зараженного объекта.
/i9	запрашивать действие 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
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
```

13.4. 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 приложения 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
```

13.5. 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>
```

13.6. Экспорт параметров защиты

Синтаксис команды:

```
avp.com EXPORT <профайл> <имя_файла>
```

Описание параметров:

<профайл>	Файловый Антивирус или задача, для которых выполняется экспорт параметров. В качестве значения параметра **<профайл>** может быть использовано любое значение, указанное в п. 13.2 на стр. 169.

<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
```

13.7. Импорт параметров

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>
```

13.8. Запуск приложения

Синтаксис команды:

```
avp.com
```

13.9. Остановка приложения

Синтаксис команды:

```
EXIT /password=<ваш_пароль>
```

<ваш_пароль>	пароль к Kaspersky Internet Security, заданный в интерфейсе приложения.
Обратите внимание, что без ввода пароля данная команда выполняться не будет.	

13.10. 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 трассировки.
[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 под-

	держки 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
```

13.11. 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>
```

13.12. 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 14. ИЗМЕНЕНИЕ, ВОССТАНОВЛЕНИЕ ИЛИ УДАЛЕНИЕ ПРИЛОЖЕНИЯ

Удалить приложение вы можете следующими способами:

- с помощью мастера установки приложения (см. п. 14.1 на стр. 183);
- из командной строки (см. п. 14.2 на стр. 186);
- 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. 36).

14.1. Изменение, восстановление и удаление приложения с помощью мастера установки

Восстановление приложения полезно проводить в том случае, если вы обнаружили какие-либо ошибки в его работе вследствие некорректной настройки или повреждения его файлов.

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 → Антивирус Касперского 6.0 для Windows Servers → 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. 26), 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.

Внимание!

При проведении удаленной деинсталляции Антивируса Касперского 6.0 автоматическая перезагрузка сервера не производится. Однако для полного удаления компонентов приложения и дальнейшей корректной работы компьютера рекомендуется произвести перезагрузку вручную.

При удалении приложения вы можете выбрать, какие данные, сформированные и используемые в работе приложения, вы хотите сохранить на сервере. 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* – информация о факте активации приложения.
- *Сигнатуры угроз* – полный набор сигнатур опасных программ, вирусов и других угроз, актуальный на дату последнего обновления.

- *Объекты резервного хранилища* – резервные копии удаленных или вылеченных объектов. Такие объекты рекомендуется сохранить для возможности последующего восстановления.
- *Объекты карантина* – объекты, возможно зараженные вирусами или их модификациями. Такие объекты содержат код, который похож на код известного вируса, но однозначно судить об их вредоносности нельзя. Рекомендуется их сохранить, поскольку они могут оказаться незараженными или их излечение будет возможно после обновления сигнатур угроз.
- *Параметры защиты* – значения параметров работы Файлового Антивируса.
- *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**.

14.2. Удаление приложения из командной строки

Для того чтобы удалить Антивирус Касперского 6.0 для Windows Servers из командной строки, наберите:

```
msiexec /x <имя_пакета>
```

Будет запущен мастер установки, с помощью которого вы сможете провести процедуру удаления приложения (см. п. Глава 14 на стр. 183).

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.

ПРИЛОЖЕНИЕ А. СПРАВОЧНАЯ ИНФОРМАЦИЯ

В данном приложении содержится справочная информация по форматам проверяемых файлов и разрешенным маскам, используемым при настройке Антивируса Касперского.

А.1. Список объектов, проверяемых по расширению

Если в качестве объектов проверки Файлового Антивируса 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:

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* – 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. 34) или Редактор объектов групповой политики (см. п. 3.4 на стр. 35). 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).

MSExclusions=yes|no – следует ли добавлять в список исключений Антивируса Касперского исключения, рекомендованные компанией Microsoft для серверов.

AddPath=yes|no – следует ли добавлять в системную переменную окружения %Path% путь к avp.com.

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

FileMonitor=yes|no – установка компонента Файловый Антивирус.

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