ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition

РУКОВОДСТВО АДМИНИСТРАТОРА

АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS SERVERS ENTERPRISE EDITION

Руководство администратора

Тел., факс: +7 (495) 797-8700, +7 (495) 645-7939,
+7 (495) 956-7000
http://www.kaspersky.ru/

Дата редакции: июль 2008 г.

Содержание

ГЛАВА 1. ВВЕДЕНИЕ

Это руководство описывает использование приложения **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** (далее – Антивирус).

В п. 1.1 на стр. 14 содержится общая информация об Антивирусе, описание его функций защиты и обнаруживаемых угроз.

Часть 1 руководства, *Настройка и управление через консоль MMC*, рассказывает о том, как управлять Антивирусом через консоль, установленную на защищаемом сервере или удаленной рабочей станции.

О том, как управлять Антивирусом из командной строки защищаемого сервера, читайте Часть 2, *Управление Антивирусом из командной строки*.

Часть 3, *Настройка и управление через Kaspersky Administration Kit*, описано централизованное управление защитой серверов, на которых установлен Антивирус, с помощью приложения Kaspersky Administration Kit.

Часть 4, *Счетчики Антивируса*, описывает счетчики Антивируса для приложения «Системный монитор», а также счетчики и ловушки SNMP.

Если вы не нашли ответа на ваш вопрос об Антивирусе в этом документе, вы можете обратиться к другим источникам информации об Антивирусе (см. п. 1.2 на стр. 21.

1.1. Общая информация об Антивирусе

Антивирус защищает серверы на платформе Microsoft Windows от угроз, проникающих посредством файлового обмена. Он предназначен для использования в локальных сетях средних и крупных организаций. Пользователями Антивируса являются администраторы сетей и сотрудники, отвечающие за антивирусную защиту сетей.

Вы можете устанавливать Антивирус на серверах, выполняющих разные функции: на серверах терминалов и принт-серверах, на серверах приложений и контроллерах доменов, а также на файловых серверах – они более других подвержены заражению, так как обмениваются файлами с рабочими станциями пользователей.

Вы можете управлять защитой сервера, на котором установлен Антивирус различными способами: с помощью консоли Антивируса в MMC, с помощью команд командной строки, а также использовать приложение Kaspersky

Administration Kit для централизованного управления защитой многих серверов, на каждом из которых установлен Антивирус. Вы можете просматривать счетчики производительности Антивируса для приложения «Системный монитор», а также счетчики и ловушки SNMP.

В этом разделе также содержится информация:

- о функциях *Постоянная защита* и *Проверка по требованию* Антивируса (см. п. 1.1.1 на стр. 15);
- об угрозах, которые обнаруживает и обезвреживает Антивирус (см. п. 1.1.2 на стр. 16);
- о том, как Антивирус обнаруживает зараженные, подозрительные и потенциально опасные объекты (см. п. 1.1.3 на стр. 20).

1.1.1. Постоянная защита и проверка по требованию

Для защиты серверов вы можете использовать две функции Антивируса: *Постоянная защита* и *Проверка по требованию*. Вы можете включать и выключать эти функции вручную и по расписанию.

Постоянная защита по умолчанию автоматически запускается при старте Антивируса и продолжает работать непрерывно.

Антивирус проверяет следующие объекты защищаемого сервера при доступе к ним:

- файлы;
- альтернативные потоки файловых систем (NTFS-streams);
- главную загрузочную запись и загрузочные секторы локальных жестких дисков и съемных носителей.

Когда какая-нибудь программа записывает на сервер или считывает с него файл, Антивирус перехватывает этот файл, проверяет его на присутствие угроз и, если обнаруживает в нем угрозу, то выполняет заданные вами действия: пытается вылечить файл или просто удаляет его. Антивирус возвращает файл программе, только если он не заражен или успешно вылечен.

Антивирус проверяет наличие в объектах не только вирусов, но и угроз других типов, например, троянских программ, программ-реклам или программ-шпионов. Подробнее об угрозах, которые обнаруживает и обезвреживает Антивирус, читайте в п. 1.1.2 на стр. 16.

Кроме этого Антивирус непрерывно отслеживает попытки выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting). Он проверяет программный код скриптов и автоматически запрещает выполнение тех из них, которые признает опасными.

Задача постоянной антивирусной защиты сервера состоит в том, чтобы обеспечить максимальную безопасность сервера при минимальном замедлении файлового обмена.

Проверка по требованию заключается в однократной полной или выборочной проверке объектов на сервере на наличие в них угроз.

Антивирус проверяет файлы, оперативную память сервера, а также объектов автозапуска, которые сложнее восстановить, если они повреждены.

По умолчанию Антивирус один раз в неделю выполняет полную проверку компьютера. Рекомендуется запускать полную проверку компьютера вручную, после того как вы отключали постоянную защиту файлов.

1.1.2. Об угрозах, которые обнаруживает Антивирус

Антивирус способен обнаруживать в файловой системе компьютера сотни тысяч различных вредоносных программ. Некоторые из этих программ представляют большую опасность для пользователя, другие опасны только при выполнении особых условий. Обнаружив вредоносную программу в объекте, Антивирус причисляет ее к определенной категории со своим уровнем опасности (высокий, средний или низкий).

Антивирус выделяет следующие категории вредоносных программ:

- вирусы и черви (Virware)
- троянские программы (Trojware);
- прочие вредоносные программы (Malware);
- программы порнографического содержания (Pornware);
- программы-рекламы (Adware);
- потенциально опасные приложения (Riskware).

Примечание

Вы можете посмотреть уровень опасности угроз в обнаруженных тельных объектах в узле **Карантин** (Глава 11 на стр. 169); уровень опасности угроз в зараженных объектах – в узле **Резервное хранилище** (Глава 12 на стр. 189).

Краткое описание угроз приводится ниже. С более подробным описанием вредоносных программ и их классификацией вы можете ознакомиться на сайте «Вирусной энциклопедии» «Лаборатории Касперского» (http://www.viruslist.com/ru/viruses/encyclopedia).

Вирусы и черви (Virware)

Уровень опасности: высокий

Эта категория включает классические вирусы и сетевые черви.

Классический вирус (класс Virus) заражает файлы других программ или данных. Он добавляет в них свой код, чтобы получить управление при их открытии. Попав в систему, классический вирус активизируется по какому-нибудь событию и выполняет свое вредоносное действие.

Классические вирусы различаются по среде обитания и способу заражения.

Под *средой обитания* понимаются области компьютера, операционные системы или приложения, в которые внедряется код вируса. По среде обитания различают файловые, загрузочные, макро- и скриптовые вирусы.

Под *способом заражения* понимаются различные методы внедрения вредоносного кода в заражаемые объекты. Существует множество разных типов вирусов по способу заражения. *Перезаписывающие* (Overwriting) вирусы записывают свой код вместо кода заражаемого файла, уничтожая его содержимое. Зараженный файл перестает работать и не восстанавливается. *Паразитические* (Parasitic) вирусы изменяют код файлов, оставляя их полностью или частично работоспособными. *Вирусы-компаньоны* (Companion) не изменяют файлы, но создают их двойники. При запуске зараженного файла управление получает его двойник, то есть вирус. Есть *вирусы-ссылки* (Link), *вирусы*, *заражающие объектные модули* (OBJ), *вирусы*, *заражающие библиотеки компиляторов* (LIB), *вирусы*, *заражающие исходные тексты программ* и другие.

Код **сетевого червя** (класс Worm), как и код классического вируса, попав в систему, активизируется и выполняет свое вредоносное действие. Но свое название сетевой червь получил благодаря способности «переползать» с компьютера на компьютер – распространять свои копии через различные информационные каналы.

Способ распространения является основным признаком, по которому сетевые черви различаются между собой. Они делятся на *почтовые*, *черви,*

использующие интернет-пейджеры, *черви в IRC-каналах*, *черви файлообменных сетей*, а также *прочие сетевые черви*. К прочим сетевым червям относятся черви, которые распространяют свои копии в сетевых ресурсах, проникают в операционные системы через уязвимости в них и в работающих в них приложениях, проникают в сетевые ресурсы публичного использования, паразитируют на других угрозах.

Многие из сетевых червей обладают очень высокой скоростью распространения.

Сетевые черви не только наносят вред зараженному компьютеру, но и дискредитируют его владельца, требуют оплаты дополнительного сетевого трафика и засоряют интернет-каналы.

Троянские программы (Trojware)

Уровень опасности: высокий

Троянские программы (классы Trojan, Backdoor, Rootkit и другие) выполняют на компьютерах действия, не санкционированные пользователем, например, воруют пароли, обращаются к интернет-ресурсам, загружают и устанавливают другие программы.

В отличие от классических вирусов, троянские программы не распространяются самостоятельно, внедряясь в файлы и заражая их. Они передаются по команде «хозяина». При этом вред, нанесенный троянской программой, может во много раз превышать вред от традиционной вирусной атаки.

Наиболее опасными среди троянских программ считаются *троянские программы удаленного администрирования* (Backdoor). При запуске такие программы устанавливают себя в системе незаметно для пользователя и выполняют скрытое управление: уничтожают данные на дисках, приводят систему к «зависанию» или передают информацию своему разработчику.

Среди троянских программ выделяют руткиты (Rootkit). Как и другие троянские программы, руткиты внедряются в систему незаметно для пользователя. Они не выполняют вредоносных действий, но скрывают другие вредоносные программы и их активность и таким образом продлевают пребывание этих программ в зараженной системе. Руткиты могут скрывать файлы, процессы в памяти зараженного компьютера или ключи реестра. Руткиты могут скрывать обращения злоумышленников к системе.

Прочие вредоносные программы (Malware)

Уровень опасности: средний

Прочие вредоносные программы не представляют угрозы компьютеру, на котором исполняются, но могут использоваться для организации сетевых атак на удаленные серверы, взлома других компьютеров, создания других вирусов или троянских программ.

Прочие вредоносные программы разнообразны. *Сетевые атаки* (класс DoS (Denial-of-Service)) посылают многочисленные запросы на удаленные серверы, что приводит к их отказу. *Злые шутки* (типы BadJoke, Hoax) пугают пользователя вирусоподобными сообщениями: они могут обнаружить вирус в незараженном файле или объявить о форматировании диска, которого на самом деле не произойдет. *Шифровальщики* (классы FileCryptor, PolyCryptor) шифруют другие вредоносные программы, чтобы скрыть их от антивирусной проверки. *Конструкторы* (класс Constructor) позволяют генерировать исходные тексты вирусов, объектные модули или зараженные файлы. *Спам-утилиты* (класс SpamTool) собирают на зараженном компьютере электронные адреса или превращают его в рассылочную спам-машину.

Программы порнографического содержания (Pornware)

Уровень опасности: средний

Программы порнографического содержания относятся к классу условно опасных программ (not-a-virus). Они обладают функциями, которые могут причинить вред пользователю только при выполнении особых условий.

Эти программы связаны с показом пользователям информации порнографического характера. В зависимости от поведения среди них выделяют три типа: *программы автодозвона* (Porn-Dialer), *программы для загрузки файлов из интернета* (Porn-Downloader) и *инструменты* (Porn-Tool). Программы автодозвона соединяются через модем с платными порнографическими интернет-ресурсами, программы для загрузки файлов из интернета загружают на компьютер порнографические материалы. К инструментам относятся программы, связанные с поиском и показом порнографических материалов (например, специальные панели инструментов для браузеров или особые видеоплееры).

Программы-рекламы (Adware)

Уровень опасности: средний

Программы-рекламы считаются условно опасными (класс not-a-virus). Их несанкционированно встраивают в другие программы для демонстрации в их интерфейсе рекламных объявлений. Многие из этих программ не только показывают рекламу, но собирают и переправляют своему разработчику персональную информацию о пользователе, изменяют параметры браузера (стартовые и поисковые страницы, уровни безопасности и т.д.), создают не контролируемый пользователем трафик. Действия программ-реклам могут привести не только к нарушению политики безопасности, но и к прямым финансовым потерям.

Потенциально опасные приложения (Riskware)

Уровень опасности: низкий

Потенциально опасные приложения относятся к классу условно опасных программ (класс not-a-virus). Такие программы могут легально продаваться и использоваться в повседневной работе, например, системных администраторов.

Потенциально опасными считаются, например, некоторые программы удаленного администрирования, такие как RemoteAdmin. Пользователь сам устанавливает и запускает эти программы на своем компьютере. Это отличает их от троянских программ удаленного администрирования Backdoor, которые сами устанавливают себя в системе и управляют ей незаметно для пользователя.

К потенциально опасным относятся также некоторые программы автоматического переключения раскладки клавиатуры, IRC-клиенты, FTP-серверы, утилиты для остановки процессов или скрытия их работы.

1.1.3. О зараженных, подозрительных и потенциально опасных объектах

Сервер, на котором установлен Антивирус, хранит набор *баз*. Базы представляют собой файлы с записями, которые позволяют идентифицировать наличие в проверяемых объектах вредоносного кода сотен тысяч известных угроз. Эти записи содержат информацию о контрольных участках кода угроз и алгоритмы лечения объектов, в которых эти угрозы содержатся.

Если Антивирус обнаруживает в проверяемом объекте участки кода, которые полностью совпадают с контрольными участками кода какой-либо угрозы в соответствии с информацией о них в базе, он признает такой объект *зараженным*, а если частично (в соответствии с определенными условиями) – *подозрительным*.

Антивирус выделяет также *потенциально опасные объекты*. Для этого он использует эвристический анализатор (Code Analyzer). Нельзя сказать, что код такого объекта частично или полностью совпадает с кодом известной угрозы, но он содержит свойственные вредоносным объектам последовательности команд, такие как открытие файла или запись в файл или перехват векторов прерываний. Эвристический анализатор определяет, например, что файл выглядит как зараженный неизвестным boot-вирусом.

Если Антивирус признает проверяемый объект зараженным или подозрительным, он возвращает название обнаруженной в нем угрозы; если Антивирус признает объект потенциально опасным, он не возвращает название угрозы в нем.

Примечание

В диалоговом окне настройки параметров безопасности и диалоговых окнах **Статистика** в консоли Антивируса термин *потенциально опасные объекты* не упоминается: Антивирус называет *подозрительными* и потенциально опасные объекты, и собственно подозрительные объекты (в коде которых обнаружены участки, частично совпадающие с кодом известных угроз).

В остальных диалоговых окнах консоли Антивируса термины *подозрительные объекты* и *потенциально опасные объекты*, упоминаются раздельно. Термин *подозрительные объекты* означает только собственно подозрительные объекты.

1.2. Получение информации об Антивирусе

Если у вас возникли вопросы по выбору, приобретению, установке или использованию Антивируса, вы можете быстро получить ответы на них.

«Лаборатория Касперского» располагает многими источниками информации о приложении, и вы можете выбрать наиболее удобный для вас в зависимости от важности и срочности вопроса. Вы можете:

- найти ответ на свой вопрос самостоятельно (см. п. 1.2.1 на стр. 22);
- получить ответ от сотрудников Департамента продаж (см. п. 1.2.2 на стр. 24);
- получить ответ от специалиста Службы технической поддержки, если вы уже приобрели Антивирус (см. п. 1.2.3 на стр. 24);
- обсудить свой вопрос не только со специалистами «Лаборатории Касперского», но и с другими пользователями в разделе вебфорума, посвященном Антивирусу (см. п. 1.2.4 на стр. 26).

1.2.1. Источники информации для самостоятельного поиска

Вы можете обратиться к следующим источникам информации о приложении:

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

Страница на веб-сайте «Лаборатории Касперского»

http://www.kaspersky.ru/Kaspersky_Anti-virus_Windows_Server_Enterprise

На этой странице вы получите общую информацию о приложении, его возможностях и особенностях. Вы можете приобрести приложение или продлить срок его использования в нашем электронном магазине.

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

http://support.kaspersky.ru/win_serv_ee_6mp2

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

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

Электронная справочная система

В комплект поставки приложения входит файл полной справки.

Полная справка содержит информацию о том, как с помощью консоли Антивируса в ММС управлять защитой компьютера: просматривать состояние защиты, выполнять проверку различных областей компьютера, выполнять другие задачи. В ней содержится информация о том, как управлять приложением из командной строки, использовать счетчики производительности Антивируса, счетчики и ловушки протокола SNMP.

Чтобы открыть полную справку, в консоли Антивируса выберите команду **Вызов справки** в меню **Справка**.

Если у вас возникнет вопрос по отдельному окну приложения, вы можете обратиться к контекстной справке.

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

Документация

Комплект документов к приложению содержит большую часть информации, необходимой для работы с ним. Он состоит из следующих документов:

- **Типовые схемы применения**. Этот документ рассказывает о применении Антивируса в сети предприятия.
- **Сравнение с Антивирусом Касперского 6.0 для Windows Servers**. Этот документ перечисляет характеристики Антивируса, которые отличают его от Антивируса Касперского 6.0 для Windows Servers.
- **Руководство по установке** содержит требования к компьютеру для установки Антивируса, инструкции по установке и активации Антивируса, проверке его работоспособности и первоначальной настройке.
- **Руководство администратора** (этот документ) содержит информацию о том, как работать с консолью Антивируса в MMC, управлять Антивирусом из приложения Kaspersky Administration Kit и из командной строки, использовать счетчики производительности Антивируса и счетчики и ловушки для протокола SNMP.

Файлы с этими документами в формате PDF входят в комплект поставки Антивируса.

Вы можете загрузить файлы документов со страницы приложения на сайте «Лаборатории Касперского».

После установки консоли Антивируса вы можете открыть руководство администратора из меню **Пуск**.

1.2.2. Обращение в Департамент продаж

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

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

Обслуживание ведется на русском и английском языках.

Вы можете задать вопрос сотрудникам Департамента продаж по электронной почте, по адресу sales@kaspersky.com.

В департаменте продаж вы можете получить консультацию по управлению защитой сети предприятия, внедрению приложения в сети или использованию его совместно с другими приложениями.

1.2.3. Обращение в Службу технической поддержки

Если вы уже приобрели приложение, вы можете получить информацию о нем от специалистов Службы технической поддержки по телефону или через интернет.

Специалисты Службы технической поддержки ответят на ваш вопрос по установке и использованию приложения и помогут устранить последствия работы вредоносных программ, если ваш компьютер уже был заражен.

Техническая поддержка по телефону

Если проблема срочная, вы всегда можете позвонить в Службу технической поддержки в нашем офисе в Москве по телефонам:

+7 (495) 797-87-07, **+7 (495) 645-79-29** или **+7 (495) 956-87-08**.

Мы оказываем техническую поддержку пользователям приложений «Лаборатории Касперского» круглосуточно, на русском и английском языках.

Если вы хотите поговорить со специалистом, который занимается именно приложением Антивирус Касперского 6.0 для Windows Servers Enterprise Edition, звоните в рабочие дни, с 10 до 18:30 часов по московскому времени (GMT +3).

Сообщите специалисту Службы технической поддержки **код активации** приложения или **серийный номер ключа** (вы можете посмотреть его узле **Ключи** консоли Антивируса, в свойствах установленного ключа).

Электронный запрос в Службу технической поддержки (для зарегистрированных пользователей)

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

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

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

Примечание

Если вы еще не являетесь зарегистрированным пользователем приложений «Лаборатории Касперского», вы можете заполнить регистрационную форму на странице:

https://support.kaspersky.com/ru/PersonalCabinet/Registration/Form/.

При регистрации укажите **код активации** приложения или **серийный номер ключа** (вы можете посмотреть его узле **Ключи** консоли Антивируса, в свойствах установленного ключа).

Вы получите ответ на свой запрос от специалиста Службы технической поддержки по электронному адресу, который вы укажете в нем, и в своем **Персональном кабинете**

https://support.kaspersky.com/ru/PersonalCabinet.

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

- **Тип запроса**. Вопросы, которые пользователи задают наиболее часто, выделены в отдельные темы, например, «Проблема установки/удаления продукта» или «Проблема поиска/удаления вирусов». Если вы не найдете подходящей темы, выберите «Общий вопрос».
- **Название продукта**: Антивирус Касперского 6.0 для Windows Servers Enterprise Edition.
- **Текст запроса**. Опишите как можно подробнее возникшую проблему.

- **Номер клиента и пароль**. Введите номер клиента и пароль, которые вы получили при регистрации на веб-сайте Службы технической поддержки.
- **Электронный адрес**. По этому адресу специалисты Службы технической поддержки перешлют ответ на ваш запрос.

1.2.4. Обсуждение приложений «Лаборатории Касперского» на веб-форуме

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

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

Вы можете, например, обсудить различные схемы внедрения приложения в организации или варианты его настройки.

ЧАСТЬ 1. НАСТРОЙКА И УПРАВЛЕНИЕ ЧЕРЕЗ КОНСОЛЬ ММС

В этой части содержится следующая информация:

- запуск консоли Антивируса в ММС, предоставление доступа к функциям Антивируса, описание внешнего вида окна консоли (Глава 2 на стр. 28);
- настройка общих параметров Антивируса (Глава 3 на стр. 46);
- импорт и экспорт параметров Антивируса и его отдельных функциональных компонентов (Глава 4 на стр. 50);
- понятие задачи в Антивирусе, типы задач, операции с задачами, настройка расписания задач, просмотр статистики задач, запуск задачи с правами другой учетной записи (Глава 5 на стр. 54);
- настройка постоянной защиты сервера (Глава 6 на стр. 67);
- блокирование доступа с компьютеров к серверу во время выполнения задачи **Постоянная защита файлов** (Глава 7 на стр. 95);
- доверенная зона (Глава 8 на стр. 108);
- настройка проверки по требованию (Глава 9 на стр. 120);
- обновление баз Антивируса и его программных модулей (Глава 10 на стр. 149);
- использование карантина для изоляции подозрительных объектов (Глава 11 на стр. 169);
- резервное копирование файлов перед их лечением или удалением, использование резервного хранилища (Глава 12 на стр. 189);
- регистрация событий и статистика Антивируса (Глава 13 на стр. 203);
- установка и удаление ключей (Глава 14 на стр. 228);
- настройка уведомлений (Глава 15 на стр. 234).

ГЛАВА 2. РАБОТА С КОНСОЛЬЮ АНТИВИРУСА В ММС И ДОСТУП К ФУНКЦИЯМ АНТИВИРУСА

В этой главе содержится следующая информация:

- о консоли Антивируса в ММС (см. п. 2.1 на стр. 28);
- дополнительная настройка после установки консоли Антивируса в ММС на другом компьютере (см. п. 2.2 на стр. 29);
- запуск консоли Антивируса из меню **Пуск** (см. п. 2.3 на стр. 35);
- функции значка Антивируса в области уведомлений панели задач защищаемого сервера (см. п. 2.4 на стр. 37);
- внешний вид окна консоли Антивируса (см. п. 2.5 на стр. 39);
- разграничение прав доступа к функциям Антивируса (см. п. 2.6 на стр. 40);
- запуск и остановка службы Антивируса (см. п. 2.7 на стр. 44).

2.1. О консоли Антивируса в ММС

Консоль Антивируса представляет собой изолированную оснастку, которая добавляется в консоль ММС (Microsoft Management Console).

При установке консоли Антивируса программа установки сохраняет файл kavfs.msc в папке Антивируса и добавляет оснастку Антивируса в список изолированных оснасток Microsoft Windows.

Вы можете открыть консоль Антивируса на защищаемом сервере, запустив ее из меню **Пуск** или из контекстного меню значка Антивируса в области уведомлений панели задач.

Вы можете запустить msc-файл оснастки Антивируса или добавить оснастку Антивируса в существующую консоль ММС как новый элемент в ее дереве. В 64-битной версии Microsoft Windows вы можете добавить оснастку

Антивируса только в ММС 32-битной версии (ММС32): откройте ММС из командной строки с помощью команды `mmc.exe /32`.

Вы можете управлять Антивирусом через консоль в ММС, установленную на защищаемом сервере или любом другом компьютере в сети. После того как вы установили консоль Антивируса на другом компьютере, вам нужно выполнить дополнительную настройку, описанную в п. 2.2 на стр. 29.

В одну консоль, открытую в авторском режиме, вы можете добавить несколько оснасток Антивируса, чтобы управлять из нее защитой нескольких серверов, на которых установлен Антивирус.

2.2. Дополнительная настройка после установки консоли Антивируса в ММС на другом компьютере

Если вы установили консоль Антивируса в ММС не на защищаемом сервере, а на другом компьютере, то для того, чтобы управлять Антивирусом на защищаемом сервере удаленно, выполните следующие действия:

- на защищаемом сервере добавьте пользователей Антивируса в группу **KAVWSEE Administrators** (см. п. 2.2.1 на стр. 30);
- если защищаемый сервер работает под управлением Microsoft Windows Server 2008, разрешите на нем сетевые соединения для файла процесса службы управления Антивирусом Касперского kavfsgt.exe (см. п. 2.2.2 на стр. 31);
- если удаленный компьютер работает под управлением Microsoft Windows XP с пакетом обновлений 1, выключите на нем брандмауэр Windows, чтобы открыть сетевые соединения для установленной на нем консоли Антивируса (см. п. 2.2.3 на стр. 32);
- для консоли Антивируса на компьютере под управлением Microsoft Windows XP с пакетом обновлений 2 или Microsoft Windows Vista: если при установке консоли вы не включили параметр **Разрешить сетевые соединения для консоли Антивируса Касперского**, то вручную разрешите сетевые соединения для консоли через брандмауэр на этом компьютере (см. п. 2.2.4 на стр. 33).

2.2.1. Добавление пользователей Антивируса в группу KAVWSEE Administrators на защищаемом сервере

Чтобы управлять Антивирусом через консоль Антивируса в MMC, установленную на другом компьютере, пользователи Антивируса должны иметь полный доступ к *службе управления Антивирусом* (*Kaspersky Anti-Virus Management*) на защищаемом сервере. По умолчанию доступ к службе имеют пользователи, входящие в группу локальных администраторов на защищаемом сервере.

Примечание

О том, какие службы регистрирует Антивирус, читайте в документе *Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство по установке*.

Вы можете предоставить доступ к службе управления Антивирусом учетным записям следующих типов:

- **учетной записи, зарегистрированной локально** на компьютере, на котором установлена консоль Антивируса. Чтобы установить соединение, на защищаемом сервере должна быть локально зарегистрирована учетная запись с такими же данными;
- **учетной записи, зарегистрированной в домене**, в котором зарегистрирован компьютер с установленной консолью Антивируса. Чтобы установить соединение, защищаемый сервер должен быть зарегистрирован или в этом же домене или в домене, который находится в доверительных отношениях с этим доменом.

Во время установки Антивирус регистрирует на защищаемом сервере группу **KAVWSEE Administrators**. Пользователям этой группы разрешен доступ к службе управления Антивирусом. Вы можете разрешать или запрещать пользователям доступ к службе управления Антивирусом, добавляя их в группу **KAVWSEE Administrators** или удаляя их из нее.

Чтобы разрешить или запретить доступ к службе управления Антивирусом:

1. На защищаемом сервере выберите **Пуск** → **Настройка** → **Панель управления**. В окне **Панель управления** выберите **Администрирование** → **Управление компьютером**.

2. В дереве консоли **Управление компьютером** разверните узел **Локальные пользователи и группы**, затем разверните узел **Группы**.
3. Дважды щелкните на группе **KAVWSEE Administrators** и в диалоговом окне **Свойства** выполните следующие действия:
   - чтобы разрешить пользователю удаленное управление Антивирусом с помощью консоли, добавьте его в группу **KAVWSEE Administrators**;
   - чтобы запретить пользователю удаленное управление Антивирусом с помощью консоли, исключите его из группы **KAVWSEE Administrators**.
4. Нажмите на кнопку **ОК** в диалоговом окне **Свойства**.

2.2.2. Разрешение на сервере под управлением Microsoft Windows Server 2008 сетевых соединений для службы управления Антивирусом Касперского

Чтобы устанавливать соединения между консолью и службой управления Антивирусом, вам нужно разрешить сетевые соединения через брандмауэр для службы управления Антивирусом Касперского на защищаемом сервере.

Чтобы разрешить сетевые соединения для службы управления Антивирусом Касперского:

1. На защищаемом сервере под управлением Microsoft Windows Server 2008 выберите **Пуск** → **Панель управления** → **Безопасность** → **Брандмауэр Windows**.
2. В окне **Параметры брандмауэра Windows** щелкните **Изменить параметры**.
3. На закладке **Исключения** в списке предустановленных исключений установите флажки **COM + Сетевой доступ**, **Windows Management Instrumentation (WMI)** и **Remote Administration**.
4. Нажмите на кнопку **Добавить программу**.

5. В диалоговом окне **Добавление программы** укажите файл kavfsgt.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке консоли Антивируса в MMC. По умолчанию полный путь к файлу следующий:

   - в Microsoft Windows 32-разрядной версии: %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 For Windows Servers Enterprise Edition\kavfsgt.exe;
   - в Microsoft Windows 64-разрядной версии: %Program-Files(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 For Windows Servers Enterprise Edition\kavfsgt.exe.

6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК** в диалоговом окне **Параметры брандмауэра Windows**.

2.2.3. Разрешение сетевых соединений для консоли Антивируса в MMC в Microsoft Windows XP с пакетом обновлений 1

Если компьютер, на котором установлена консоль Антивируса, работает под управлением Microsoft Windows XP с пакетом обновлений 1, вам нужно отключить брандмауэр Windows на этом компьютере, чтобы разрешить сетевые соединения для консоли:

1. На компьютере, на котором установлена консоль Антивируса в MMC, выберите **Пуск** → **Панель управления** → **Сетевые подключения**.
2. Откройте контекстное меню на названии сетевого подключения (например, **Local Area Connection**) и выберите команду **Свойства**.
3. В диалоговом окне **<Название сетевого подключения>: Свойства** на закладке **Дополнительно** снимите флажок **Защитить мое подключение к Интернету**.
4. Нажмите на кнопку **ОК**.

2.2.4. Разрешение сетевых соединений для консоли Антивируса в ММС в Microsoft Windows XP с пакетом обновлений 2 или Microsoft Windows Vista

Консоль Антивируса в ММС на удаленном компьютере использует протокол DCOM, чтобы получать информацию о событиях Антивируса (проверенных объектах, завершении задач и др.) от службы управления Антивирусом на защищаемом сервере.

Если компьютер, на котором установлена консоль, работает под управлением Microsoft Windows XP с пакетом обновлений 2 или Microsoft Windows Vista, вам нужно разрешить сетевые соединения через брандмауэр на этом компьютере, чтобы устанавливать соединения между консолью и службой управления Антивирусом.

Выполните следующие действия:

- убедитесь, что разрешен анонимный удаленный доступ к приложениям COM (но не удаленный запуск и активация приложений COM) и
- в брандмауэре Windows откройте порт TCP 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Антивирусом kavfsrcn.exe.

  Через порт TCP 135 клиентский компьютер, на котором установлена консоль Антивируса в ММС, обменивается информацией с защищаемым сервером.

Чтобы разрешить анонимный удаленный доступ к приложениям COM:

1. На компьютере, на котором установлена консоль Антивируса в ММС, откройте консоль **Службы компонентов**: выберите **Пуск** → **Выполнить**, введите **dcomcnfg** и нажмите на кнопку **ОК**.
2. В консоли **Службы компонентов** компьютера разверните узел **Компьютеры**, откройте контекстное меню на узле **Мой компьютер** и выберите команду **Свойства**.
3. В диалоговом окне **Свойства** на закладке **Безопасность COM** нажмите на кнопку **Изменить ограничения** в группе параметров **Права доступа**.

4. В диалоговом окне **Разрешение на доступ** убедитесь, что для пользователя **ANONYMOUS LOGON** установлен флажок **Разрешить удаленный доступ**.
5. Нажмите на кнопку **ОК**.

Чтобы открыть в брандмауэре Windows TCP-порт 135 и разрешить сетевые соединения для исполняемого файла процесса удаленного управления Антивирусом:

1. На удаленном компьютере закройте консоль Антивируса в MMC.
2. Выполните одно из следующих действий:
   - в *Microsoft Windows XP с пакетом обновлений 2 или выше* выберите **Пуск → Панель управления → Брандмауэр Windows**.
   - в *Microsoft Windows Vista* выберите **Пуск → Панель управления → Брандмауэр Windows** и в окне **Брандмауэр Windows** щелкните **Изменить параметры**.
3. В диалоговом окне **Брандмауэр Windows** (**Параметры брандмауэра Windows**) на закладке **Исключения** нажмите на кнопку **Добавить порт**.
4. В поле **Имя** укажите имя порта **RPC(TCP/135)** или задайте другое имя, например, **DCOM Антивируса**, в поле **Номер порта** укажите номер порта: **135**.
5. Выберите протокол **TCP**.
6. Нажмите на кнопку **ОК**.
7. На закладке **Исключения** нажмите на кнопку **Добавить программу**.
8. В диалоговом окне **Добавление программы** укажите файл kavfsrcn.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке консоли Антивируса в MMC. По умолчанию полный путь к файлу следующий:
   - *в Microsoft Windows 32-разрядной версии*: %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe;
   - *в Microsoft Windows 64-разрядной версии*: %Program-Files(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe.
9. Нажмите на кнопку **ОК**.

10. Нажмите на кнопку **ОК** в диалоговом окне **Брандмауэр Windows** (**Параметры брандмауэра Windows**).

> **Примечание**
>
> *Чтобы применить новые параметры соединения*: если консоль Антивируса была открыта, когда вы выполняли настройку соединения между защищаемым сервером и компьютером, на котором она установлена, закройте консоль, подождите 30-60 секунд (пока завершится процесс удаленного управления Антивирусом kavfsrcn.exe), а затем снова запустите ее.

2.3. Запуск консоли Антивируса из меню *Пуск*

Убедитесь, что консоль Антивируса установлена на компьютере.

*Чтобы запустить консоль Антивируса из меню **Пуск**:*

1. Выберите **Пуск** → **Программы** → **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** → **Средства администрирования** → **Консоль Антивируса Касперского**.

> **Примечание**
>
> Если вы планируете добавлять в консоль Антивируса другие оснастки, откройте консоль в авторском режиме: выберите **Пуск** → **Программы** → **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** → **Средства администрирования**, откройте контекстное меню на приложении **Консоль Антивируса Касперского** и выберите команду **Автор**.

Если вы запустили консоль Антивируса на защищаемом сервере, откроется окно консоли (см. рис. 1).

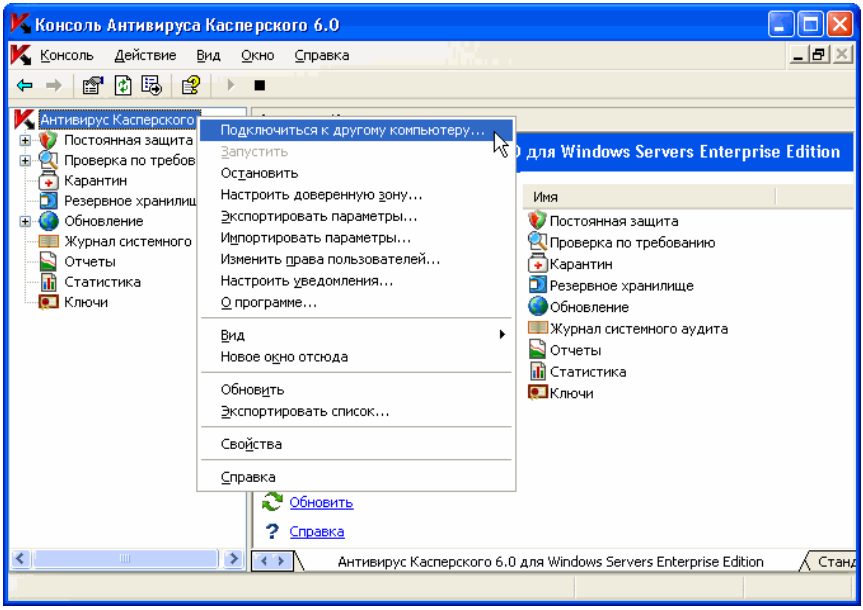

Рисунок 1. Окно консоли Антивируса

2. Если вы запустили консоль Антивируса не на защищаемом сервере, а на другом компьютере, подключитесь к защищаемому серверу: откройте контекстное меню на названии оснастки Антивируса, выберите команду **Подключиться к другому компьютеру**, затем в диалоговом окне **Выбор компьютера** выберите **Другой компьютер** и в поле ввода укажите сетевое имя защищаемого сервера.

   Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе управления Антивирусом на сервере, укажите другую учетную запись, которая обладает этими правами. Подробнее о том, каким учетным записям вы можете предоставлять доступ к службе управления Антивирусом, читайте в п. 2.2.1 на стр. 30.

2.4. Значок Антивируса в области уведомлений панели задач

Каждый раз когда Антивирус автоматически запускается после перезагрузки сервера, в области уведомлений панели задач отображается значок Антивируса . Он отображается по умолчанию, если при установке Антивируса вы включили в набор устанавливаемых компонентов компонент **Приложение панели задач**.

Значок Антивируса может иметь одно из следующих состояний:

- активный (цветной), если в текущий момент выполняется какая-либо из задач постоянной защиты: **Постоянная защита файлов** или **Проверка скриптов** (подробнее о задачах постоянной защиты читайте в п. 6.1 на стр. 67);
- неактивный (черно-белый), если в текущий момент задачи **Постоянная защита файлов** и **Проверка скриптов** не выполняются.

Щелкнув на значке Антивируса правой клавишей мыши, вы откроете контекстное меню, показанное на рис. 2.

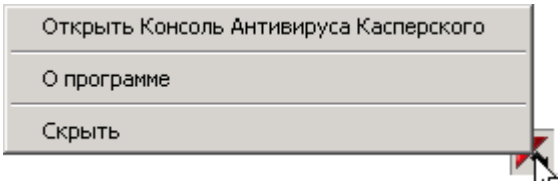

Рисунок 2. Контекстное меню значка Антивируса

Контекстное меню имеет следующие команды:

Команда	Описание
Открыть консоль Антивируса Касперского	Открывает консоль Антивируса в ММС (если она установлена).

Команда	Описание
О программе	Открывает окно **О программе** с информацией об Антивирусе. Если вы зарегистрированы в качестве пользователя Антивируса, то окно **О программе** содержит информацию об установленных срочных обновлениях.
Скрыть	Скрывает значок Антивируса в области уведомлений панели задач. Чтобы отобразить значок Антивируса, в меню **Пуск** выберите **Программы** → **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** → **Приложение панели задач**.

В настройках общих параметров Антивируса вы можете включить или выключить отображение значка Антивируса при автоматическом запуске Антивируса после перезагрузки сервера (см. п. 3.2 на стр. 46).

2.5. Окно консоли Антивируса

Окно консоли Антивируса (см. рис. 3) содержит дерево консоли и панель результатов. В дереве консоли отображаются узлы функциональных компонентов Антивируса, в панели результатов отображается информация о выбранном узле.

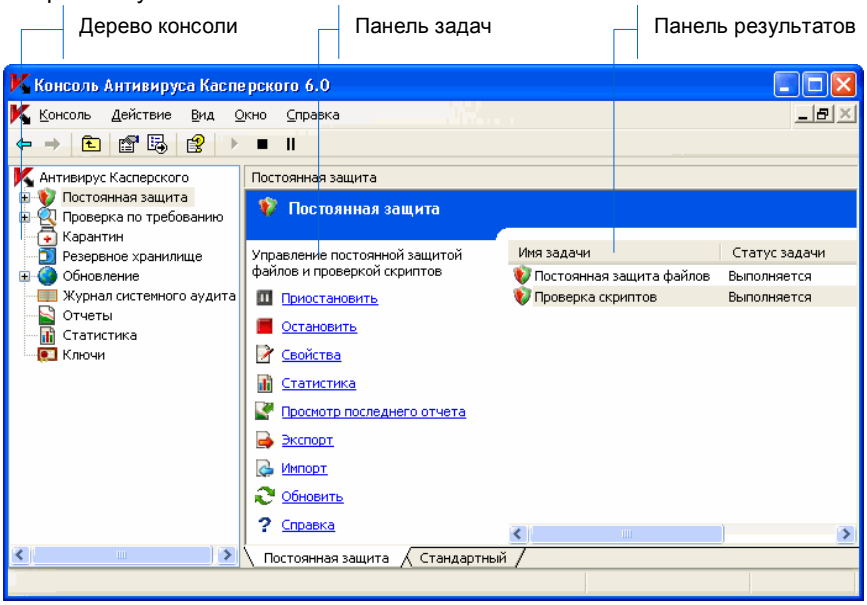

Рисунок 3. Консоль Антивируса

Окно консоли Антивируса содержит также панель задач, если вы запустили консоль из меню **Пуск** (из msc-файла, сохраненного при установке Антивируса). Если вы добавили оснастку Антивируса в существующую консоль ММС, то консоль не содержит панели задач.

2.6. Разграничение прав доступа к функциям Антивируса

Этот раздел содержит следующую информацию:

- о правах доступа к функциям Антивируса (см. п. 2.6.1 на стр. 40);
- предоставление прав доступа к функциям Антивируса (см. п. 2.6.2 на стр. 42).

2.6.1. О правах доступа к функциям Антивируса

По умолчанию доступ ко всем функциям Антивируса имеют пользователи группы **Администраторы** и пользователи группы **KAVWSEE Administrators**, созданной на защищаемом сервере при установке Антивируса.

Пользователи, которые имеют доступ к функции **Изменение прав** Антивируса, могут предоставлять доступ к функциям Антивируса другим пользователям, зарегистрированным на защищаемом сервере или входящим в домен.

Если пользователь не зарегистрирован в списке пользователей Антивируса, он не сможет просматривать консоль Антивируса в ММС.

Вы можете предоставлять пользователям Антивируса (группе пользователей) права доступа:

- ко всем функциям Антивируса (**полный контроль**);
- ко всем функциям Антивируса кроме функции управления правами пользователей (**изменение**);
- только на просмотр функциональных компонентов Антивируса, общих параметров Антивируса, параметров его функций и задач, статистики и прав пользователей (**чтение**).

Вы также можете выполнять расширенную настройку прав доступа: разрешать или запрещать доступ к отдельным функциям Антивируса. Функции, доступом к которым вы можете управлять, перечислены в таблице 1.

Таблица 1. Разграничение прав доступа к функциям Антивируса

Функция	**Описание**
Чтение статистики	Просмотр состояния функциональных компонентов Антивируса и статистики выполняющихся задач
Управление состоянием задачи	Запуск / остановка / приостановка / возобновление задач Антивируса
Управление задачами	Создание и удаление задач проверки по требованию
Чтение параметров	• Просмотр общих параметров Антивируса и параметров задач; • просмотр параметров отчетов, уведомлений и системного аудита; • экспорт параметров Антивируса
Изменение параметров	• Просмотр и изменение общих параметров Антивируса; • импорт и экспорт параметров Антивируса; • просмотр и изменение параметров задач; • просмотр и изменение параметров отчетов, уведомлений и журнала системного аудита
Управление хранилищами	• Помещение объектов на карантин; • удаление объектов из карантина и файлов из резервного хранилища; • восстановление объектов из резервного хранилища и карантина
Чтение отчетов	Просмотр сводных и подробных отчетов о выполнении задач в узле **Отчеты** и событий в узле **Журнал системного аудита**
Управление отчетами	Удаление отчетов и очистка журнала системного аудита
Управление ключами	Установка и удаление ключей
Чтение прав	Просмотр списка пользователей Антивируса

Функция	Описание
Изменение прав	• Добавление и удаление пользователей Антивируса; • изменение прав доступа пользователей к функциям Антивируса

2.6.2. Настройка прав доступа к функциям Антивируса

Чтобы добавить или удалить пользователя (группу) или изменить права доступа пользователя (группы):

1. В дереве консоли откройте контекстное меню на названии оснастки Антивируса и выберите **Изменить права пользователей**.

   Откроется диалоговое окно **Разрешения** (см. рис. 4).

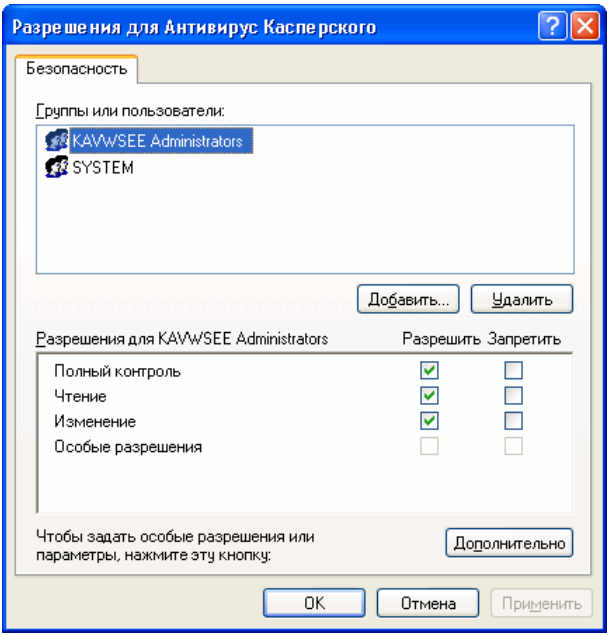

Рисунок 4. Диалоговое окно **Разрешения**

2. В диалоговом окне **Разрешения** выполните следующие действия:

   - чтобы добавить пользователя (группу) в список пользователей Антивируса, нажмите на кнопку **Добавить** и выберите пользователей или группы, которых вы хотите добавить;

   - чтобы предоставить добавленному пользователю (группе) права доступа к функциям Антивируса, выберите пользователя (группу) под заголовком **Группы или пользователи** и под заголовком **Разрешения для <Пользователь (Группа)>** установите флажок **Разрешить** для следующих прав доступа:

     - **Полный контроль**, чтобы предоставить доступ ко всем функциям Антивируса;

     - **Чтение**, чтобы предоставить доступ к функциям **Чтение статистики**, **Чтение параметров**, **Чтение отчетов** и **Чтение прав**;

     - **Изменение**, чтобы предоставить доступ ко всем функциям Антивируса кроме функции **Изменение прав**;

   - чтобы выполнить расширенную настройку прав (**Особые разрешения**), нажмите на кнопку **Дополнительно**, в диалоговом окне **Дополнительные параметры безопасности** выберите нужного пользователя или группу и нажмите на кнопку **Изменить**, а затем в диалоговом окне **Элемент разрешения** (см. рис. 5) установите флажок **Разрешить** или **Запретить** рядом с названиями функций, доступ к которым вы хотите разрешить или запретить (список функций и их краткое описание приводится в таблице 1). Нажмите на кнопку **ОК**.

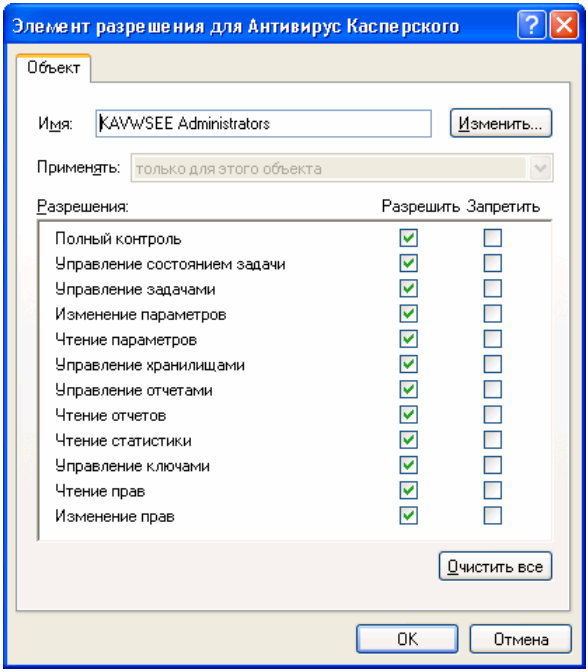

Рисунок 5. Диалоговое окно **Элемент разрешения**

3. Нажмите на кнопку **OK** в диалоговом окне **Разрешения**.

2.7. Запуск и остановка службы Антивируса

По умолчанию служба Антивируса запускается автоматически при запуске операционной системы. Служба Антивируса управляет рабочими процессами, в которых выполняются задачи постоянной защиты, проверки по требованию и обновления.

По умолчанию при запуске службы Антивируса запускаются задачи **Постоянная защита файлов**, **Проверка скриптов**, **Проверка при старте системы** и **Проверка целостности приложения**, а также другие задачи, в расписании которых указана частота запуска **При запуске приложения**.

Если вы остановите службу Антивируса, все выполняющиеся задачи будут прерваны. После того как вы снова запустите службу Антивируса, они не

будут автоматически возобновлены. Только задачи, в расписании которых указана частота запуска **При запуске приложения**, будут запущены снова.

Примечание

Вы можете запускать и останавливать службу Антивируса, только если вы входите в группу локальных администраторов на защищаемом сервере.

Чтобы остановить или запустить службу Антивируса, в дереве консоли откройте контекстное меню на названии оснастки Антивируса и выберите одну из следующих команд:

- **Остановить**, чтобы остановить службу Антивируса;
- **Запустить**, чтобы запустить службу Антивируса.

Вы также можете запускать и останавливать службу Антивируса через оснастку **Службы** Microsoft Windows.

ГЛАВА 3. ОБЩИЕ ПАРАМЕТРЫ АНТИВИРУСА

В этой главе содержится следующая информация:

- об общих параметрах Антивируса (см. п. 3.1 на стр. 46);
- настройка общих параметров Антивируса (см. п. 3.2 на стр. 46).

Описание общих параметров Антивируса приводится в п. A.1 на стр. 372.

3.1. Об общих параметрах Антивируса

Общие параметры Антивируса устанавливают общие условия работы Антивируса. Они позволяют регулировать количество рабочих процессов, используемых Антивирусом, включать восстановление задач Антивируса после их аварийного завершения, вести журнал трассировки, включать создание дампов памяти процессов Антивируса при их аварийном завершении, включать или выключать отображение значка Антивируса при автоматическом запуске Антивируса после перезагрузки сервера и др.

3.2. Настройка общих параметров Антивируса

В этом разделе содержится информация о том, как настраивать общие параметры Антивируса. Описание общих параметров приводится в п. A.1 на стр. 372.

Чтобы настроить общие параметры Антивируса:

1. В дереве консоли откройте контекстное меню на названии оснастки Антивируса и выберите команду **Свойства**.
2. На следующих закладках измените значения общих параметров Антивируса согласно вашим требованиям:
   - На закладке **Общие** (см. рис. 6):

- установите максимальное количество рабочих процессов, которые Антивирус может запустить (см. п. A.1.1 на стр. 373);
- установите фиксированное количество процессов для задач постоянной защиты (см. п. A.1.2 на стр. 374);
- установите количество рабочих процессов для фоновых задач проверки по требованию (см. п. A.1.3 на стр. 376);
- задайте количество попыток восстановления задач после их аварийного завершения (см. п. A.1.4 на стр. 377).

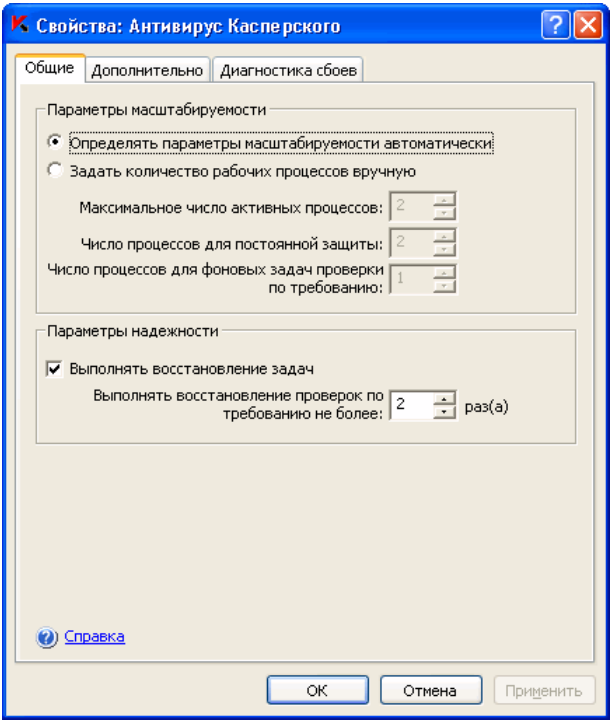

Рисунок 6. Диалоговое окно **Свойства: Антивирус Касперского**, закладка **Общие**

- На закладке **Дополнительно** (см. рис. 7):
  - укажите, отображать ли значок Антивируса в области уведомлений панели задач сервера каждый раз при запуске Антивируса после перезагрузки сервера (подробнее о значке Антивируса читайте в п. 2.4 на стр. 37)

- укажите, сколько дней будут храниться сводные и подробные отчеты о выполнении задач, которые отображаются в узле **Отчеты** консоли Антивируса (см. п. A.1.5 на стр. 378);
- укажите, сколько дней будет храниться информация, которая отображается в узле **Журнал системного аудита** (см. п. A.1.6 на стр. 379);
- укажите действия Антивируса при работе от источника бесперебойного питания (см. п. A.1.7 на стр. 379);
- установите пороговое количество дней, после которого будут возникать события *Базы устарели*, *Базы сильно устарели* и *Полная проверка компьютера выполнялась давно* (см. п. A.1.8 на стр. 380).

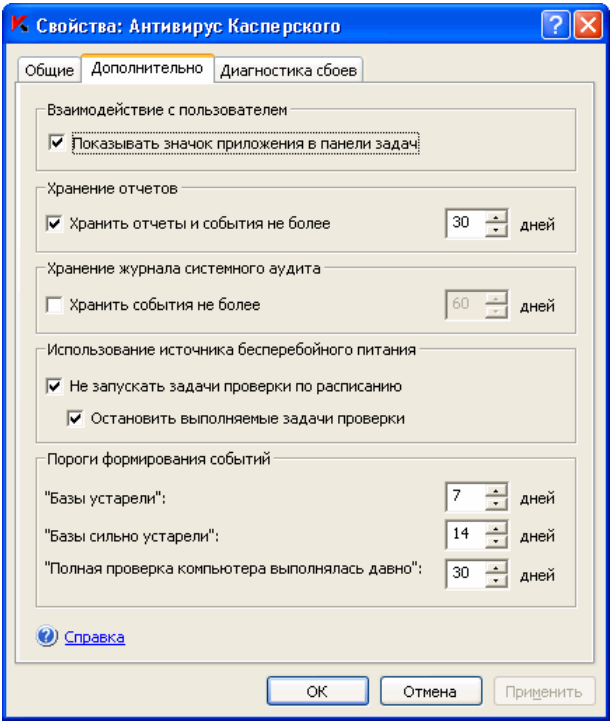

Рисунок 7. Диалоговое окно **Свойства: Антивирус Касперского**, закладка **Дополнительно**

- На закладке **Диагностика сбоев** (см. рис. 8):
  - включите или выключите создание журнала трассировки; если требуется, настройте параметры журнала (см. п. A.1.9 на стр. 381);
  - включите или выключите создание файлов дампов памяти процессов Антивируса (см. п. A.1.10 на стр. 388).

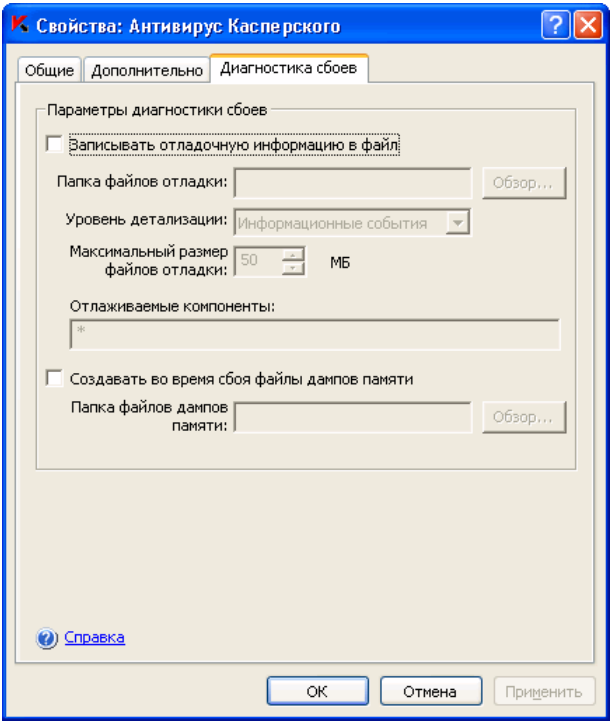

Рисунок 8. Диалоговое окно **Свойства: Антивирус Касперского**, закладка **Диагностика сбоев**

3. После того как вы измените значения нужных общих параметров Антивируса, нажмите на кнопку **OK**.

ГЛАВА 4. ИМПОРТ И ЭКСПОРТ ПАРАМЕТРОВ АНТИВИРУСА

В этой главе содержится следующая информация:

4.1. Об импорте и экспорте параметров

Если вам нужно установить одинаковые значения параметров Антивируса на нескольких защищаемых серверах, вы можете настроить параметры Антивируса на одном из серверов, экспортировать их в конфигурационный файл в формате XML, а затем импортировать их из этого файла в Антивирус на других серверах.

Вы можете сохранить в конфигурационный файл как все параметры Антивируса, так и параметры отдельных функциональных компонентов.

Когда вы экспортируете все параметры Антивируса, Антивирус сохраняет в файл общие параметры Антивируса и параметры следующих функциональных компонентов:

- Постоянная защита файлов;
- Проверка скриптов;
- Блокирование доступа с компьютеров;
- Проверка по требованию;
- Обновление баз и модулей Антивируса;
- Карантин;
- Резервное хранилище;
- Отчеты;

- Уведомления;
- Доверенная зона;

а также сохраняет права учетных записей пользователей.

Антивирус не экспортирует параметры групповых задач и список блокирования доступа с компьютеров.

Антивирус экспортирует все используемые в нем пароли, например, данные учетных записей для запуска задач или соединения с прокси-сервером, сохраняя их в конфигурационном файле в зашифрованном виде. Но импортировать их может только Антивирус на этом же компьютере, если он не был переустановлен или обновлен. Антивирус на другом компьютере их не импортирует. После импорта параметров на другом компьютере вам нужно ввести все пароли вручную.

Если в момент экспорта параметров действует политика приложения Kaspersky Administration Kit, то Антивирус экспортирует не значения, применяемые политикой, а значения действующие до ее применения.

Примечание

Импортируемые параметры задач не применяются в выполняющихся задачах, а применяются только при запуске задач. Рекомендуется остановить задачи в функциональных компонентах перед импортом в них параметров.

4.2. Экспорт параметров

Чтобы экспортировать параметры в конфигурационный файл:

1. Если вы изменяли параметры в консоли Антивируса, то перед экспортом параметров нажмите на кнопку **Сохранить**, чтобы сохранить их новые значения.
2. Выполните одно из следующих действий:
   - чтобы экспортировать все параметры Антивируса, в окне консоли откройте контекстное меню на названии оснастки Антивируса и выберите команду **Экспортировать параметры**;
   - чтобы экспортировать параметры отдельного функционального компонента, в дереве консоли откройте контекстное меню на узле этого функционального компонента и выберите команду **Экспортировать параметры**.

   Откроется окно приветствия мастера экспорта параметров.

3. Выполните инструкции в окнах мастера: задайте имя конфигурационного файла, в котором вы хотите сохранить параметры, и путь к файлу.

   Указывая путь, вы можете использовать системные переменные окружения, вы не можете использовать пользовательские переменные окружения.

   Примечание

   Если в момент экспорта параметров действует политика приложения Kaspersky Administration Kit, то Антивирус экспортирует не значения, применяемые политикой, а значения действующие до ее применения.

4. В окне **Экспорт завершен** нажмите на кнопку **ОК**, чтобы закрыть мастер экспорта параметров.

4.3. Импорт параметров

Чтобы импортировать параметры из конфигурационного файла:

1. Выполните одно из следующих действий:

   - чтобы импортировать все параметры Антивируса, в дереве консоли откройте контекстное меню на названии оснастки Антивируса и выберите команду **Импортировать параметры**;
   - чтобы импортировать параметры отдельного функционального компонента, в дереве консоли откройте контекстное меню на узле этого функционального компонента и выберите команду **Импортировать параметры**.

   Откроется окно приветствия мастера импорта параметров.

2. Выполните инструкции в окнах мастера: укажите конфигурационный файл, из которого вы хотите импортировать параметры.

   Примечание

   После того как вы импортируете общие параметры Антивируса или его функциональных компонентов на сервере, вы не сможете вернуть их прежние значения.

3. В окне **Импорт завершен** нажмите на кнопку **ОК**, чтобы закрыть мастер импорта параметров.

4. В консоли Антивируса, в панели инструментов, нажмите на кнопку **Обновить**  , чтобы отобразить импортированные параметры.

> **Примечание**
>
> Антивирус не импортирует пароли (данные учетных записей для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом компьютере или на том же компьютере, после того как на нем переустановили или обновили Антивирус. После завершения импорта вам нужно ввести пароли вручную.

ГЛАВА 5. УПРАВЛЕНИЕ ЗАДАЧАМИ

В этой главе содержится следующая информация:

5.1. Категории задач Антивируса

Функции *Постоянная защита*, *Проверка по требованию*, *Обновление* и *Управление ключами* Антивируса реализованы в виде *задач*. Вы можете запускать и останавливать задачи вручную и по расписанию.

По месту создания и выполнения задачи делятся на *локальные* и *групповые*. Локальные задачи бывают двух категорий: *системные* и *пользовательские*.

Локальные задачи

Локальные задачи выполняются только на том защищаемом сервере, для которого они созданы.

- **Локальные системные задачи** создаются автоматически при установке Антивируса. Вы можете изменять параметры всех системных задач, кроме задач **Проверка объектов на карантине**, **Про-**

верка целостности приложения и **Откат обновления баз**. Вы не можете переименовывать или удалять системные задачи. Вы можете запускать системные и пользовательские задачи проверки по требованию одновременно.

- **Локальные пользовательские задачи**. В консоли Антивируса в ММС вы можете добавлять новые задачи проверки по требованию. В Консоли администрирования приложения Kaspersky Administration Kit вы можете создавать новые задачи проверки по требованию, обновления баз, отката обновления баз и копирования обновлений. Эти задачи называются пользовательскими. Вы можете переименовывать, настраивать и удалять пользовательские задачи. Вы можете запускать несколько пользовательских задач одновременно.

Групповые задачи

Групповые и глобальные задачи, созданные в Консоли администрирования Kaspersky Administration Kit, отображаются в консоли Антивируса в ММС. Все они называются в консоли Антивируса групповыми. Вы можете управлять групповыми задачами и настраивать их из приложения Kaspersky Administration Kit. В консоли Антивируса в ММС вы можете только просматривать состояние групповых задач.

В консоли Антивируса отображается информация о задачах (см. пример на рис. 9).

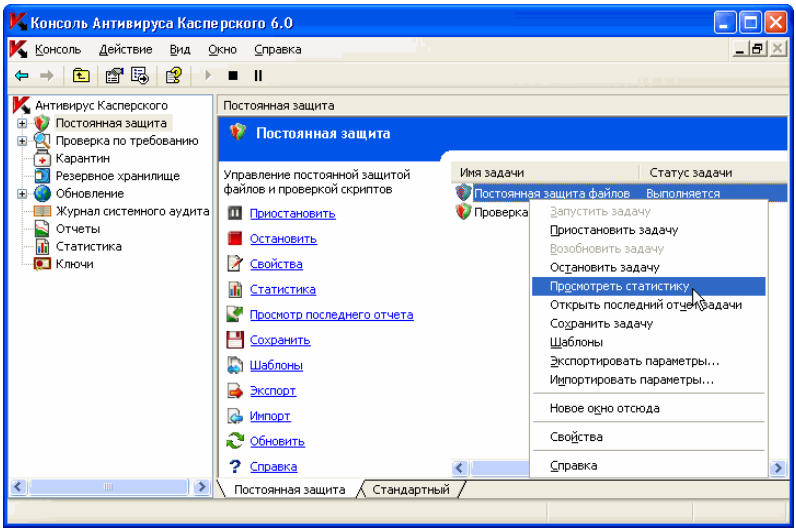

Рисунок 9. Задачи постоянной защиты в окне консоли Антивируса

Команды управления задачей отображаются в контекстном меню, которое открывается по щелчку правой клавишей мыши на имени задачи.

Операции по управлению задачами регистрируются в журнале системного аудита (см. п. 13.3 на стр. 217).

5.2. Создание задачи

Вы можете создавать пользовательские задачи в узле **Проверка по требованию**. В других функциональных компонентах Антивируса создание пользовательских задач не предусмотрено.

Чтобы создать новую задачу проверки по требованию:

1. В дереве консоли откройте контекстное меню на узле **Проверка по требованию** и выберите команду **Добавить задачу** (см. рис. 10).

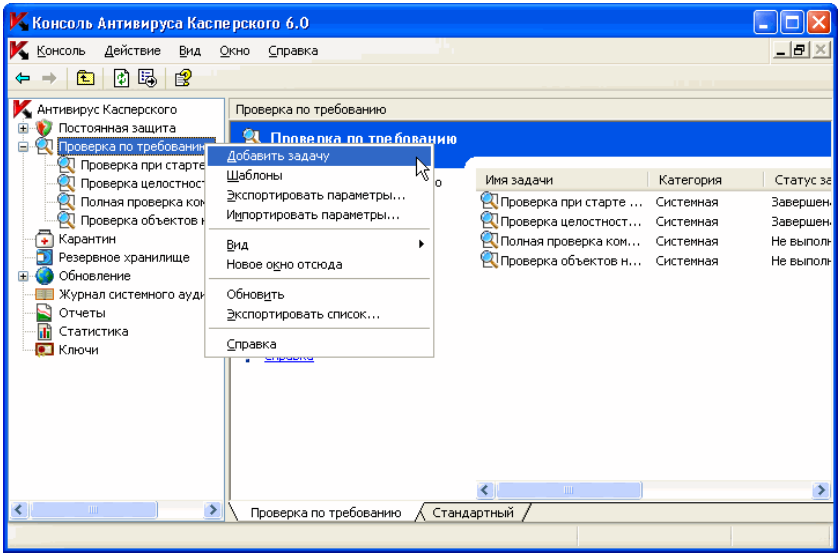

Рисунок 10. Пример создания задачи

Откроется диалоговое окно **Создание задачи** (см. рис. 11).

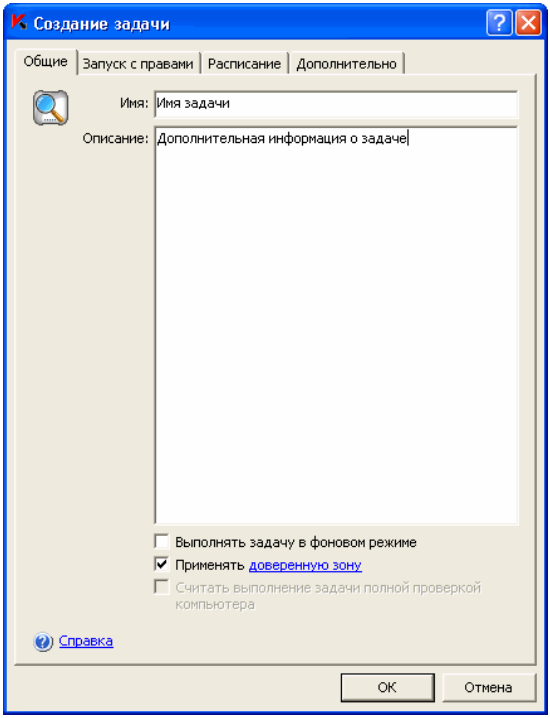

Рисунок 11. Диалоговое окно **Создание задачи**

2. Введите следующую информацию о задаче:
   - **Имя** – имя задачи, не более 100 символов;
   - **Описание** – любая дополнительная информация о задаче, не более 2000 символов. Эта информация отображается в диалоговом окне свойств задачи.
3. Если требуется выполнять задачу в процессе с низким приоритетом, установите флажок **Выполнять задачу в фоновом режиме** (подробнее о приоритетах задач Антивируса читайте в п. 9.3 на стр. 143).
4. Нажмите на кнопку **ОК**. Задача будет создана. Строка с информацией о ней появится в окне консоли.

5.3. Сохранение задачи после изменения ее параметров

Вы можете изменять параметры как выполняемой, так и остановленной (приостановленной) задачи:

- *если вы изменили параметры выполняемой задачи*: в задачах постоянной защиты новые значения параметров начнут использоваться сразу после того, как вы их сохраните; в остальных задачах они применятся при следующем запуске задачи;
- *если вы изменили параметры остановленной задачи*: новые значения параметров начнут использоваться после того, как вы сохраните их и запустите задачу.

Чтобы сохранить измененные параметры задачи, откройте контекстное меню на имени задачи и выберите команду ***Сохранить задачу****.*

Примечание

Если после изменения параметров задачи вы выберете другой узел дерева консоли, не выбрав предварительно команду **Сохранить задачу**, то появится диалоговое окно сохранения параметров. В нем нажмите на кнопку **Да**, чтобы сохранить параметры задачи, или **Нет**, чтобы покинуть узел без их сохранения.

О том, как настроить параметры задачи **Постоянная защита файлов**, читайте в п. 6.2 на стр. 68.

О том, как настроить параметры задач проверки по требованию, читайте в п. 9.2 на стр. 121.

Настройка параметров задач обновления описана в п. 10.5 на стр. 158.

5.4. Переименование задачи

Вы можете переименовывать только пользовательские задачи в консоли Антивируса; вы не можете переименовывать системные или групповые задачи.

Чтобы переименовать задачу:

1. Откройте контекстное меню на имени задачи и выберите команду **Свойства**.

2. В диалоговом окне **Свойства задачи** введите новое имя задачи в поле **Имя** и нажмите на кнопку **ОК**.

Задача будет переименована. Операция будет зарегистрирована в журнале системного аудита (см. п. 13.3 на стр. 217).

О том, как настроить расписание задачи, см. п. 5.7 на стр. 60.

5.5. Удаление задачи

Вы можете удалять только пользовательские задачи в консоли Антивируса; вы не можете удалять системные или групповые задачи.

Чтобы удалить задачу:

1. Откройте контекстное меню на имени задачи и выберите команду **Удалить задачу**.
2. В диалоговом окне **Удаление задачи** нажмите на кнопку **Да**, чтобы подтвердить операцию.

Задача будет удалена, операция удаления будет зарегистрирована в журнале системного аудита (см. п. 13.3 на стр. 217).

5.6. Запуск / приостановка / возобновление / остановка задачи вручную

Вы можете приостанавливать и возобновлять все задачи, кроме задач обновления.

Чтобы запустить / приостановить / возобновить / остановить задачу, откройте контекстное меню на имени задачи и выберите нужную команду: ***Запустить задачу***, ***Приостановить задачу***, ***Возобновить задачу*** *или* ***Остановить задачу***.

Операция будет выполнена. В панели результатов изменится статус задачи; операция будет зарегистрирована в журнале системного аудита (см. п. 13.3 на стр. 217).

Примечание

Когда вы приостановите и возобновите задачу проверки по требованию, Антивирус продолжит проверку с того объекта, на котором выполнение задачи было приостановлено.

5.7. Работа с расписанием задач

В этом разделе содержится следующая информация:

- настройка расписания задачи (см. п. 5.7.1 на стр. 60);
- включение / выключение настроенного расписания задачи (см. п. 5.7.2 на стр. 63).

Параметры расписания описаны в п. A.2 на стр. 390.

5.7.1. Настройка расписания задачи

В консоли Антивируса вы можете настраивать расписание локальных системных и пользовательских задач. Вы не можете настраивать расписание групповых задач.

Описание параметров расписания приводится в п. A.2 на стр. 390.

Чтобы настроить параметры расписания задачи:

1. Откройте контекстное меню на имени задачи, расписание которой вы хотите настроить, и выберите **Свойства**.
2. В диалоговом окне **Свойства задачи** (см. рис. 12) на закладке **Расписание** включите запуск задачи по расписанию: установите флажок **Запускать задачу по расписанию**.

   Примечание

   Поля с параметрами расписания системной задачи недоступны, если ее запуск по расписанию запрещен действием политики приложения Kaspersky Administration Kit (см. п. 19.4 на стр. 294).

3. Настройте параметры расписания в соответствии с вашими требованиями.

   а) Укажите частоту запуска задачи (см. п. A.2.1 на стр. 390): в списке **Частота запуска** выберите одно из следующих значений: **Ежечасно**, **Ежедневно**, **Еженедельно**, **При запуске Антивируса**, **При обновлении баз**:

- если вы выбрали **Ежечасно**, укажите количество часов в поле **Каждые <количество> часов** в группе параметров **Параметры запуска задачи**;
- если вы выбрали **Ежедневно**, укажите количество дней в поле **Каждые <количество> дней** в группе параметров **Параметры запуска задачи**;
- если вы выбрали **Еженедельно**, укажите количество недель в поле **Каждые <количество> недель** в группе параметров **Параметры запуска задачи**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам);

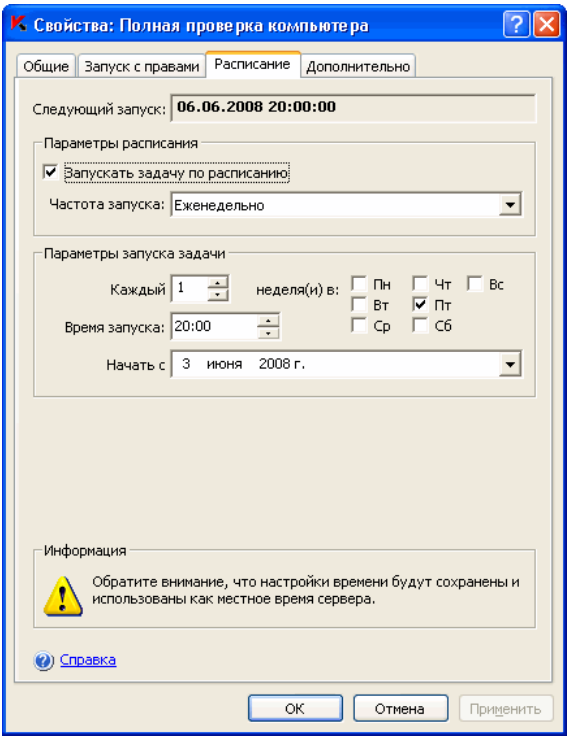

Рисунок 12. Пример закладки **Расписание** со значением **Частоты запуска**: **Еженедельно**

б) В поле **Время запуска** укажите время первого запуска задачи.

в) В поле **Начать с** укажите дату начала действия расписания (см. п. A.2.2 на стр. 392).

Примечание

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части диалогового окна в поле **Следующий запуск** появится информация о *расчетном времени очередного запуска задачи*. Обновленная информация о расчетном времени следующего запуска будет отображаться каждый раз, когда вы откроете диалоговое окно **Свойства задачи** на закладке **Расписание**.

Значение **Запуск задачи запрещен политикой** в поле **Следующий запуск** отображается, если запуск системных задач по расписанию запрещен параметрами действующей политики приложения Kaspersky Administration Kit (подробнее читайте в п. 19.4 на стр. 294).

4. На закладке **Дополнительно** (см. рис. 13) настройте в соответствии с вашими требованиями остальные параметры расписания.

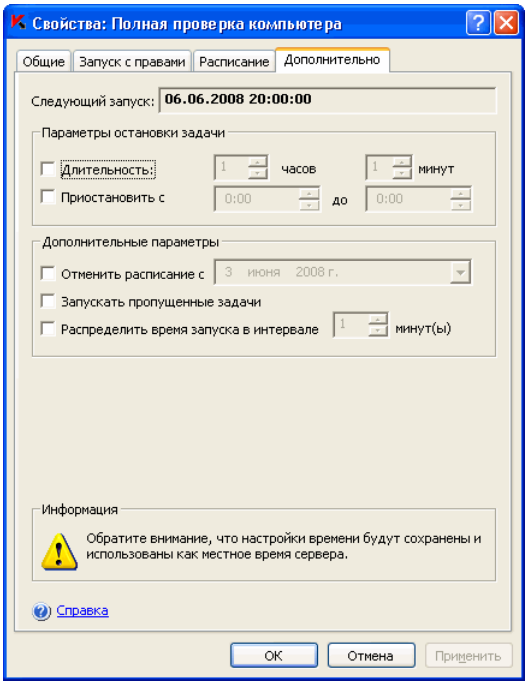

Рисунок 13. Диалоговое окно **Свойства задачи**, закладка **Дополнительно**

а) Чтобы указать максимальную длительность выполнения задачи, в группе **Параметры остановки задачи** в поле **Длительность** введите нужное количество часов и минут (см. п. A.2.4 на стр. 394).

б) Чтобы указать промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено, в группе **Параметры остановки задачи** введите начальное и конечное значение промежутка в поле **Приостановить с … до** (см. п. A.2.5 на стр. 395).

в) Чтобы указать дату, начиная с которой расписание перестанет действовать, установите флажок **Отменить расписание с** и с помощью диалогового окна **Календарь** выберите дату, начиная с которой расписание перестанет действовать (см. п. A.2.3 на стр. 393).

г) Чтобы включить запуск пропущенных задач, установите флажок **Запускать пропущенные задачи** (см. п. A.2.6 на стр. 396).

д) Чтобы включить использование параметра **Распределение времени запуска**, установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах (см. п. A.2.7 на стр. 397).

5. Нажмите на кнопку **ОК**, чтобы сохранить изменения в диалоговом окне **Свойства задачи**.

5.7.2. Включение и выключение запуска по расписанию

Настроив расписание задачи, вы можете включать и выключать его. После того как вы выключите расписание, его параметры (частота запуска, время запуска и другие) не будут удалены, и вы сможете снова включить расписание, когда потребуется.

Чтобы включить или выключить расписание:

1. Откройте контекстное меню на имени задачи, расписание которой вы хотите включить или выключить, и выберите команду **Свойства**.

2. В диалоговом окне **Свойства задачи** на закладке **Расписание** выполните одно из следующих действий:

   - чтобы включить расписание, установите флажок **Запускать задачу по расписанию**;

- чтобы выключить расписание, снимите флажок **Запускать задачу по расписанию**.

3. Нажмите на кнопку **ОК**.

5.8. Просмотр статистики задачи

Пока задача выполняется, вы можете просматривать подробную информацию о ее выполнении с момента запуска по текущий момент в диалоговом окне **Статистика**.

Информация в диалоговом окне **Статистика** будет доступна, если вы приостановите задачу. После завершения или остановки задачи вы сможете просмотреть эту информацию в подробном отчете о событиях в задаче (см. п. 13.2.4 на стр. 209).

Чтобы просмотреть статистику задачи, в окне консоли откройте контекстное меню на имени задачи, статистику которой вы хотите просмотреть, и выберите команду ***Просмотреть статистику****.*

5.9. Использование учетных записей для запуска задач

В этом разделе содержится следующая информация:

- об использовании учетных записей для запуска задач (см. п. 5.9.1 на стр. 64);
- указание учетной записи для запуска задачи (см. п. 5.9.2 на стр. 65).

5.9.1. Об использовании учетных записей для запуска задач

Вы можете указать учетную запись, с правами которой будет запускаться выбранная задача любого функционального компонента Антивируса, кроме компонента **Постоянная защита**.

По умолчанию все задачи, кроме задач постоянной защиты, выполняются под учетной записью **Локальная система** (**SYSTEM**). В задачах постоянной защиты Антивирус перехватывает проверяемый объект, когда к нему обра-

щается какое-нибудь приложение; он использует для доступа к объекту права этого приложения.

Вам нужно указать другую учетную запись с достаточными правами доступа в следующих случаях:

- в задаче обновления, если в качестве источника обновления вы указали папку общего доступа на другом компьютере в сети;
- в задаче обновления, если для доступа к источнику обновлений используется прокси-сервер со встроенной проверкой подлинности Microsoft Windows (NTLM-authentication);
- в задачах проверки по требованию, если учетная запись **Локальная система** (**SYSTEM**) не обладает правами доступа к каким-либо из проверяемых объектов (например, к файлам в папках общего доступа в сети).

Примечание

Вы можете запускать под учетной записью **Локальная система** (**SYSTEM**) задачи обновления и проверки по требованию, в которых Антивирус обращается к папкам общего доступа на другом компьютере в сети, если этот компьютер зарегистрирован в одном домене с защищаемым сервером. В этом случае учетная запись **Локальная система** (**SYSTEM**) должна обладать правами доступа к этим папкам. Антивирус будет обращаться к компьютеру с правами учетной записи **Имя_домена\имя_компьютера$**.

5.9.2. Указание учетной записи для запуска задачи

Чтобы указать учетную запись для запуска задачи:

1. Откройте контекстное меню на имени задачи и выберите команду **Свойства**.
2. В диалоговом окне **Свойства задачи** откройте закладку **Запуск с правами** (см. рис. 14).

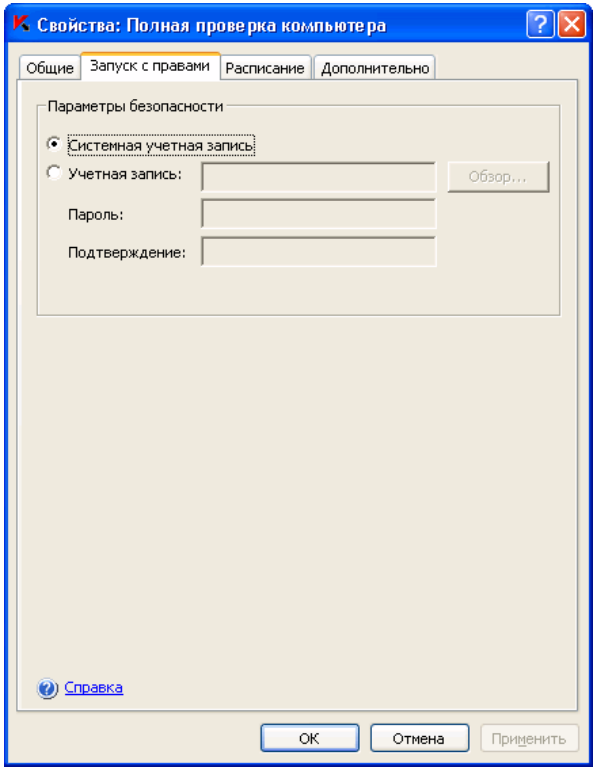

Рисунок 14. Диалоговое окно **Свойства задачи**, закладка **Запуск с правами**

3. На закладке **Запуск с правами** выполните следующие действия:

   а) Выберите **Учетная запись**.

   б) Укажите имя и пароль пользователя, учетную запись которого вы хотите использовать.

   Примечание

   Выбранный вами пользователь должен быть зарегистрирован на защищаемом сервере или в одном домене с ним.

   в) Нажмите на кнопку **ОК**.

ГЛАВА 6. ПОСТОЯННАЯ ЗАЩИТА

В этой главе содержится следующая информация:

- о задачах постоянной защиты (см. п. 6.1 на стр. 67);
- настройка задачи **Постоянная защита файлов** (см. п. 6.2 на стр. 68);
- статистика задачи **Постоянная защита файлов** (см. п. 6.3 на стр. 90);
- настройка задачи **Проверка скриптов**: выбор действий над подозрительными скриптами (см. п. 6.4 на стр. 92);
- статистика задачи **Проверка скриптов** (см. п. 6.5 на стр. 94);

6.1. О задачах постоянной защиты

В Антивирусе предусмотрены две системные задачи постоянной защиты: **Постоянная защита файлов** и **Проверка скриптов**. Подробнее о функции *Постоянная защита* читайте в п. 1.1.1 на стр. 15.

По умолчанию задачи постоянной защиты автоматически запускаются при старте Антивируса. Вы можете останавливать и снова запускать эти задачи и / или настроить их расписание. Вы также можете приостановить и возобновить задачу постоянной защиты, если требуется прервать проверку объектов при доступе на короткое время, например на время репликации данных.

Вы можете настраивать задачу **Постоянная защита файлов** – формировать область защиты и устанавливать параметры безопасности для выбранных узлов, настраивать блокирование доступа с компьютеров, применять доверенную зону (см. п. 6.2 на стр. 68).

Когда выполняется задача **Проверка скриптов**, Антивирус контролирует выполнение скриптов, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), например, скриптов VBScript или JScript. Антивирус запрещает выполнение скриптов, которые он признает опасными. Если Антивирус признает скрипт подозрительным, то он выполняет выбранное вами действие: запрещает или разрешает его выполнение. О том, как разрешить или запретить выполнение подозрительных скриптов, см. п. 6.4 на стр. 92.

6.2. Настройка задачи *Постоянная защита файлов*

По умолчанию системная задача **Постоянная защита файлов** имеет параметры, описанные в таблице 2. Вы можете изменять значения этих параметров – настраивать задачу.

Таблица 2. Параметры задачи **Постоянная защита файлов** по умолчанию

Параметр	Значение по умолчанию	Описание
Область защиты	Весь сервер	Вы можете ограничить область защиты (см. п. 6.2.1 на стр. 71).
Параметры безопасности	Единые для всей области защиты; соответствуют уровню безопасности **Рекомендуемый**.	Для выбранных узлов в дереве файловых ресурсов сервера вы можете: • применить другой предустановленный уровень безопасности (см. п. 6.2.2.1 на стр. 78); • вручную изменить параметры безопасности (см. п. 6.2.2.2 на стр. 82). Вы можете сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла (см. п. 6.2.2.3 на стр. 85).
Режим защиты объектов	При открытии и изменении	Вы можете выбрать режим защиты объектов – при каком типе доступа к объектам Антивирус проверяет их. О том, как выбрать режим защиты объектов, читайте в п. 6.2.3 на стр. 89. Подробнее о режимах защиты объектов читайте в п. A.3.1 на стр. 399.

Параметр	Значение по умолчанию	Описание
Блокирование доступа с компьютеров	Выключено	Вы можете блокировать доступ с компьютеров к защищаемому серверу при попытке записи на сервер зараженных или подозрительных объектов (Глава 7 на стр. 95).
Доверенная зона	Применяется Исключаются программы удаленного администрирования **RemoteAdmin** и файлы, рекомендованные корпорацией Microsoft, если при установке Антивируса вы выбрали **Добавить к исключениям угрозы по маске not-a-virus:RemoteAdmin*** и **Добавить к исключениям файлы, рекомендованные Microsoft**.	Единый список исключений, который вы можете применять в выбранных задачах проверки по требованию и задаче **Постоянная защита файлов**. Глава 8 на стр. 108 содержит информацию о создании и применении доверенной зоны.

*Чтобы настроить задачу **Постоянная защита файлов**:*

1. В дереве консоли разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.

   В панели результатов отобразится дерево файловых ресурсов сервера и диалоговое окно **Уровень безопасности** (Стандартный режим) (см. рис. 15).

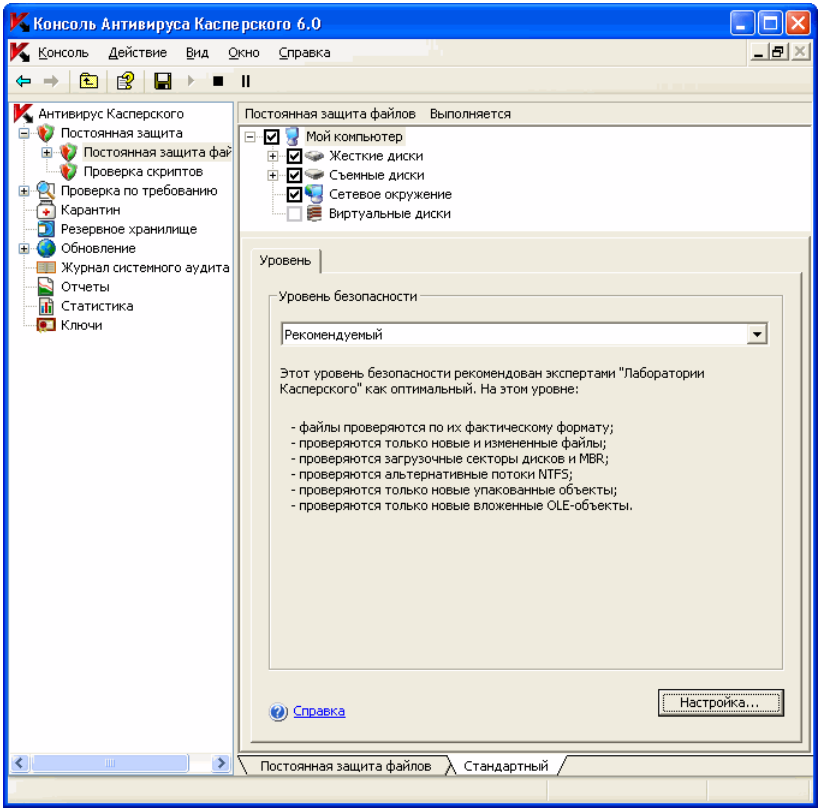

Рисунок 15. Открыта задача **Постоянная защита файлов**

3. Настройте нужные параметры задачи.
4. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

О том, как:

- запустить / приостановить / возобновить / остановить задачу вручную, см. п. 5.6 на стр. 59.
- запустить задачу по расписанию, см. п. 5.7 на стр. 60.

6.2.1. Область защиты в задаче *Постоянная защита файлов*

В этом разделе содержится информация:

- о формировании области защиты в задаче *Постоянная защита файлов* (см. п. 6.2.1.1 на стр. 71);
- о том, какие предопределенные области сервера вы можете включать в область защиты (см. п. 6.2.1.2 на стр. 72);
- о том, как сформировать область защиты: исключить из нее или включить в нее отдельные области сервера (см. п. 6.2.1.3 на стр. 73);
- о виртуальной области защиты – дисках, папках и файлах, которые монтируются на сервер временно, а также папках и файлах, которые динамически создаются на сервере различными приложениями и службами (см. п. 6.2.1.4 на стр. 74);
- о том, как создать виртуальную область защиты (см. п. 6.2.1.5 на стр. 75).

6.2.1.1. О формировании области защиты в задаче *Постоянная защита файлов*

Если задача **Постоянная защита файлов** выполняется с параметрами, установленными по умолчанию, Антивирус проверяет все объекты файловой системы сервера. Если по требованиям к безопасности вам нет необходимости проверять их все, вы можете ограничить область защиты.

В консоли Антивируса область защиты представляет собой дерево файловых ресурсов сервера, которые Антивирус может проверять.

Узлы дерева файловых ресурсов сервера отображаются следующим образом:

☑ Узел включен в область защиты.

☐ Узел исключен из области защиты.

☑ По крайней мере один из узлов, вложенных в этот узел, исключен из области защиты или параметры безопасности вложенного узла (узлов) отличаются от параметров безопасности этого узла.

Обратите внимание, что родительский узел будет отмечен значком ☑, если вы выберете все вложенные узлы, но не сам родительский узел. В этом случае файлы и папки, которые появятся в этом узле, не будут автоматически включены в область защиты. Чтобы включить их, вы можете включить в область защиты их родительский узел. Или вы можете создать их «виртуальные копии» в консоли Антивируса и добавить их в область защиты.

Имена виртуальных узлов области защиты отображаются шрифтом синего цвета.

6.2.1.2. Предопределенные области защиты

Когда вы откроете задачу **Постоянная защита файлов**, в панели результатов отобразится дерево файловых ресурсов сервера (см. рис. 16).

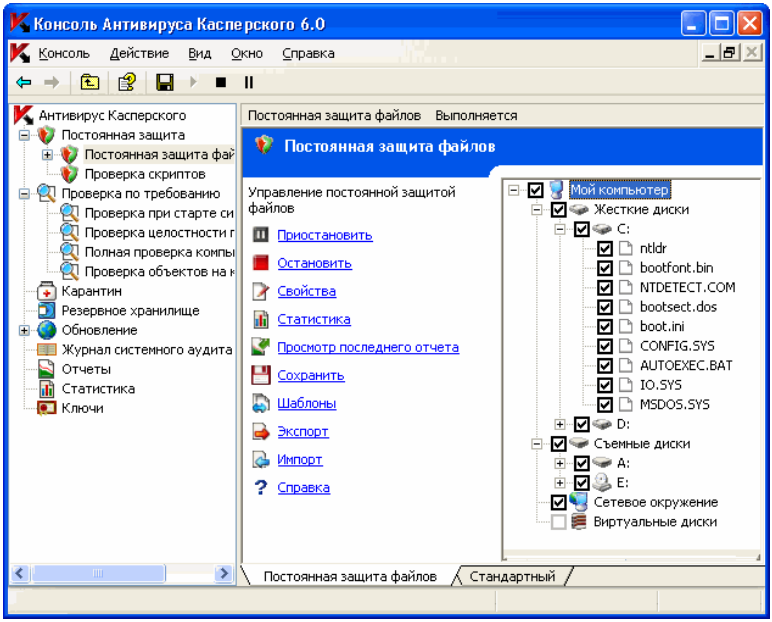

Рисунок 16. Пример дерева файловых ресурсов сервера в консоли Антивируса

Примечание

Дерево файловых ресурсов отображает узлы, к которым у вас есть доступ на чтение в соответствии с настройками безопасности Microsoft Windows.

Дерево файловых ресурсов сервера содержит следующие предопределенные области защиты:

- **Жесткие диски**. Антивирус проверяет файлы на жестких дисках сервера.
- **Съемные диски**. Антивирус проверяет файлы на сменных носителях, например, компакт-дисках или USB-накопителях.
- **Сетевое окружение**. Антивирус проверяет файлы, которые записываются в сетевые папки или считываются из них приложениями, выполняющимися на сервере. Антивирус не проверяет файлы в сетевых папках, когда к ним обращаются приложения с других компьютеров.
- **Виртуальные диски**. Вы можете включать в область защиты динамические папки и файлы, а также диски, которые монтируются на сервер временно, например, общие диски кластера (создать *виртуальную область защиты*).

Примечание

Псевдодиски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов сервера в консоли Антивируса. Чтобы включить в область защиты объекты на псевдодиске, включите в область защиты папку на сервере, с которой этот псевдодиск связан.

Подключенные сетевые диски также не отображаются в дереве файловых ресурсов сервера. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

6.2.1.3. Формирование области защиты

Чтобы сформировать область защиты:

1. Откройте задачу **Постоянная защита файлов**.
2. В панели результатов, в дереве файловых ресурсов сервера, выполните следующие действия:
   - чтобы исключить из области защиты отдельный узел, разверните дерево файловых ресурсов, чтобы отобразить нужный узел, и снимите флажок рядом с именем узла.
   - чтобы выбрать только те узлы, которые вы хотите включить в область защиты, снимите флажок **Мой компьютер**, а затем:

- если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с названием нужного типа дисков (например, чтобы включить все съемные диски на сервере, установите флажок **Съемные диски**);
- если вы хотите включить в область защиты отдельный диск нужного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**;
- если вы хотите включить в область защиты только отдельную папку на диске, разверните дерево файловых ресурсов сервера, чтобы отобразить папку, которую вы хотите включить в область защиты, и установите флажок рядом с ее именем. Таким же образом вы можете включать в область защиты и файлы.

3. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

Примечание

Вы сможете запустить задачу **Постоянная защита файлов**, только если по крайней мере один узел дерева файловых ресурсов сервера включен в область защиты.

Примечание

Если вы укажете сложную область защиты, например, установите различные значения параметров безопасности для многих отдельных узлов в дереве файловых ресурсов сервера, это может привести к некоторому замедлению проверки объектов при доступе.

6.2.1.4. О виртуальной области защиты

Антивирус может проверять не только существующие папки и файлы на жестких и сменных дисках, но и диски, которые монтируются на сервер временно, например, общие диски кластера, а также папки и файлы, которые динамически создаются на сервере различными приложениями и службами.

Если вы включили в область защиты все объекты сервера, то эти динамические узлы автоматически войдут в область защиты. Однако, если вы хотите задать специальные значения параметров безопасности для этих динамических узлов или вы выбрали для постоянной защиты не весь сервер,

а отдельные области, то для того, чтобы включить в область защиты динамические диски, файлы или папки, вам нужно предварительно создать их в консоли Антивируса – задать *виртуальную область защиты*. Созданные вами диски, файлы и папки существуют только в консоли Антивируса, но не в структуре файловой системы защищаемого сервера.

Если, формируя область защиты, вы выберете все вложенные папки или файлы, но не выберете родительскую папку, то динамические папки или файлы, которые появятся в ней, не будут автоматически включены в область защиты. Вам нужно создать их «виртуальные копии» в консоли Антивируса и добавить их в область защиты.

О том, как создать виртуальную область защиты в задаче **Постоянная защита файлов**, см. п. 6.2.1.5 на стр. 75.

О том, как создавать виртуальную область защиты в задачах проверки по требованию, см. п. 9.2.1.5 на стр. 128.

6.2.1.5. Создание виртуальной области защиты: включение в область защиты динамических дисков, папок и файлов

Чтобы добавить в область защиты виртуальный диск:

1. В дереве консоли разверните узел **Постоянная защита** и выберите вложенный узел **Постоянная защита файлов**.
2. В панели результатов, в дереве файловых ресурсов сервера, откройте контекстное меню на узле **Виртуальные диски** и в списке доступных имен выберите имя для создаваемого виртуального диска (см. рис. 17).

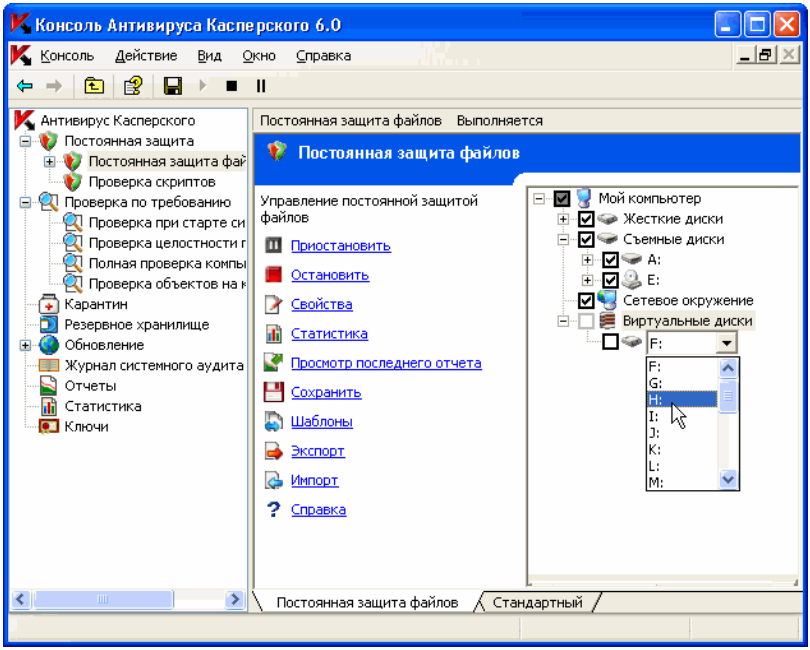

Рисунок 17. Выбор имени для создаваемого виртуального диска

3. Установите флажок рядом с добавленным диском, чтобы включить этот диск в область защиты.

4. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

Чтобы добавить в область защиты виртуальную папку или виртуальный файл:

1. В дереве консоли разверните узел **Постоянная защита** и выберите вложенный узел **Постоянная защита файлов**.

2. В панели результатов, в дереве файловых ресурсов сервера, откройте контекстное меню на узле, в который вы хотите добавить папку или файл, и выберите **Добавить виртуальную папку** или **Добавить виртуальный файл**.

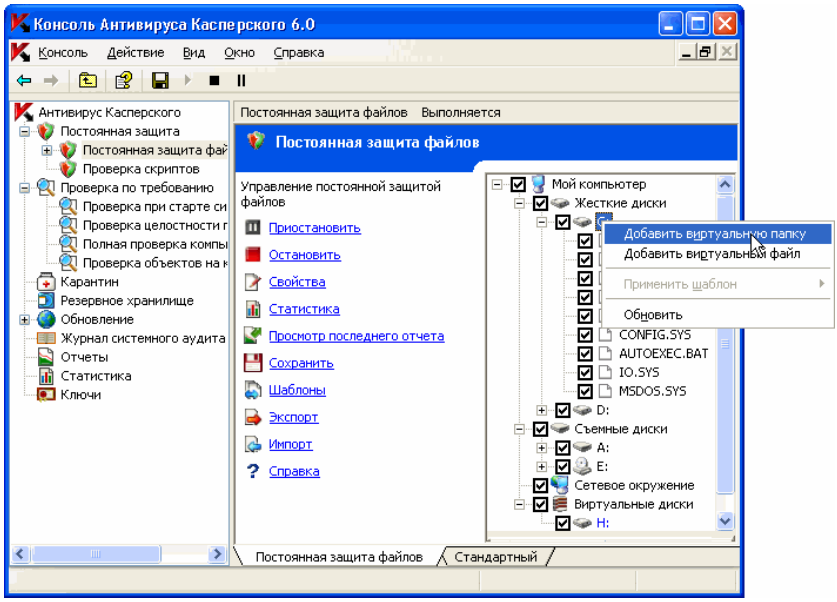

Рисунок 18. Добавление виртуальной папки

3. В поле ввода задайте имя для папки (файла). Указывая имя файла, вы можете задать его маску с помощью специальных символов * и ?.

4. В строке с названием созданной папки (созданного файла) установите флажок, чтобы включить папку (файл) в область защиты.

5. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

6.2.2. Настройка параметров безопасности выбранного узла

Вы можете настроить параметры безопасности выбранного узла в дереве файловых ресурсов сервера следующим образом:

- выбрать один из трех предустановленных уровней безопасности (максимальная скорость, рекомендуемый или максимальная защита) (см. п. 6.2.2.1 на стр. 78);

- вручную изменить параметры безопасности выбранного узла (см. п. 6.2.2.2 на стр. 82).

Вы можете сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применять этот шаблон для других узлов (см. п. 6.2.2.3 на стр. 85).

6.2.2.1. Выбор предустановленных уровней безопасности в задаче *Постоянная защита файлов*

Для выбранных узлов в дереве файловых ресурсов сервера вы можете применить один из следующих предустановленных уровней безопасности: а) максимальная скорость, б) рекомендуемый и с) максимальная защита. Каждый из этих уровней имеет свой набор значений параметров безопасности. Значения параметров предустановленных уровней безопасности приведены в таблице 3 на стр. 79.

Максимальная скорость

Вы можете установить уровень безопасности **Максимальная скорость** на сервере, если в вашей сети, кроме использования Антивируса на серверах и рабочих станциях, принимаются дополнительные меры компьютерной безопасности, например, настроены сетевые экраны, действуют политики безопасности для пользователей сети.

Рекомендуемый

Уровень безопасности **Рекомендуемый** установлен по умолчанию. Он признан специалистами «Лаборатории Касперского» достаточным для защиты файловых серверов в большинстве сетей. Этот уровень обеспечивает оптимальное сочетание качества защиты и степени влияния на производительность защищаемых серверов.

Максимальная защита

Используйте уровень безопасности **Максимальная защита**, если вы предъявляете повышенные требования к компьютерной безопасности в сети.

Таблица 3. Предустановленные уровни безопасности и соответствующие им значения параметров безопасности

Параметры	Уровень безопасности		
	Максимальная скорость	**Рекомендуемый**	**Максимальная защита**
Проверяемые объекты (см. п. А.3.2 на стр. 400)	По расширению	По формату	По формату
Проверка только новых и измененных объектов (см. п. А.3.3 на стр. 402)	Включена	Включена	Выключена
Действие над зараженными объектами (см. п. А.3.5 на стр. 404)	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно
Действие над подозрительными объектами (см. п. А.3.6 на стр. 407)	Помещать на карантин	Помещать на карантин	Помещать на карантин
Исключение объектов (см. п. А.3.8 на стр. 411)	Нет	Нет	Нет
Исключение угроз (см. п. А.3.9 на стр. 412)	Нет	Нет	Нет
Максимальная продолжительность проверки объекта (см. п. А.3.10 на стр. 414)	60 сек.	60 сек.	60 сек.
Максимальный размер проверяемого составного объекта (см. п. А.3.11 на стр. 415)	8 МБ	8 МБ	Не установлен

Параметры	Уровень безопасности		
	Максимальная скорость	**Рекомендуемый**	**Максимальная защита**
Проверка дополнительных потоков файловой системы (NTFS) (см. п. A.3.2 на стр. 400)	Да	Да	Да
Проверка загрузочных секторов (см. п. A.3.2 на стр. 400)	Да	Да	Да
Проверка составных объектов (см. п. A.3.4 на стр. 403)	Упакованные объекты* * Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты

Примечание

Обратите внимание, что параметры безопасности **Режим защиты объектов**, **Применение технологии iChecker** и **Применение технологии iSwift** не входят в набор параметров предустановленных уровней безопасности. По умолчанию они включены. Если, выбрав один из предустановленных уровней безопасности, вы измените состояние параметров безопасности **Режим защиты объектов**, **Применение технологии iChecker** или **Применение технологии iSwift**, выбранный вами предустановленный уровень безопасности не изменится.

Чтобы выбрать один из предустановленных уровней безопасности:

1. В дереве консоли разверните узел **Постоянная защита** и выберите вложенный узел **Постоянная защита файлов**.

2. В панели результатов, в дереве файловых ресурсов сервера, выберите узел, для которого вы хотите выбрать предустановленный уровень безопасности.

3. Убедитесь, что этот узел включен в область защиты (см. п. 6.2.1.3 на стр. 73).

4. В диалоговом окне **Уровень безопасности** (см. рис. 19) выберите уровень безопасности, который вы хотите применить, в списке **Уровень безопасности**.

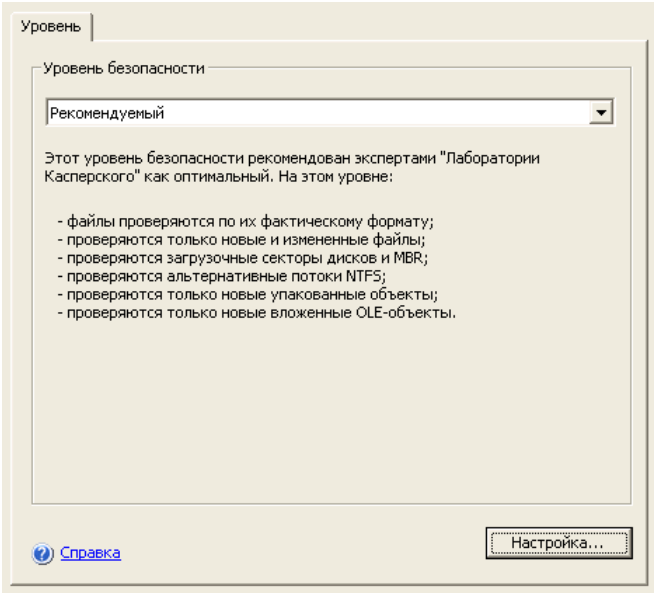

Рисунок 19. Диалоговое окно **Уровень безопасности**

В диалоговом окне отобразится список значений параметров безопасности, соответствующих выбранному вами уровню безопасности.

5. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

6.2.2.2. Настройка параметров безопасности вручную

По умолчанию в задаче **Постоянная защита файлов** применяются единые параметры безопасности для всей области защиты. Их значения соответствуют значениям предустановленного уровня безопасности **Рекомендуемый**. Значения параметров безопасности, установленных по умолчанию, приводятся в п. 6.2.2.1 на стр. 78.

Вы можете изменять значения параметров безопасности по умолчанию, настроив их как едиными для всей области защиты, так и различными для разных узлов в дереве файловых ресурсов сервера.

Параметры безопасности, которые вы настроите для выбранного узла, будут автоматически применяться для всех узлов, вложенных в него. Однако, если вы отдельно настроите параметры безопасности для вложенного узла, то параметры безопасности родительского узла не будут для него применяться.

Чтобы вручную настроить параметры безопасности выбранного узла:

1. В дереве консоли разверните узел **Постоянная защита** и выберите вложенный узел **Постоянная защита файлов**.
2. В панели результатов, в дереве файловых ресурсов сервера, выберите узел, параметры безопасности которого вы хотите настроить.
3. Нажмите на кнопку **Настройка** в нижней части диалогового окна.

   Откроется диалоговое окно **Параметры безопасности**.

   Примечание

   О том, как применить шаблон параметров безопасности для узла, см. п. 6.2.2.3 на стр. 85.

4. Настройте нужные параметры безопасности выбранного узла в соответствии с вашими требованиями:

   - На закладке **Общие** (см. рис. 20) выполните следующие действия:
     - под заголовком **Защита объектов** укажите, будет ли Антивирус проверять все объекты области защиты или только объекты определенных форматов или с определенными расширениями, будет ли Антивирус проверять загрузочные секторы дисков и главную загрузочную запись, альтернативные потоки NTFS (см. п. А.3.2 на стр. 400);

- под заголовком **Оптимизация** укажите, будет ли Антивирус проверять все объекты в выбранной области или только новые и измененные (см. п. А.3.3 на стр. 402);
- под заголовком **Защита составных объектов** укажите, какие составные объекты Антивирус будет проверять (см. п. А.3.4 на стр. 403).

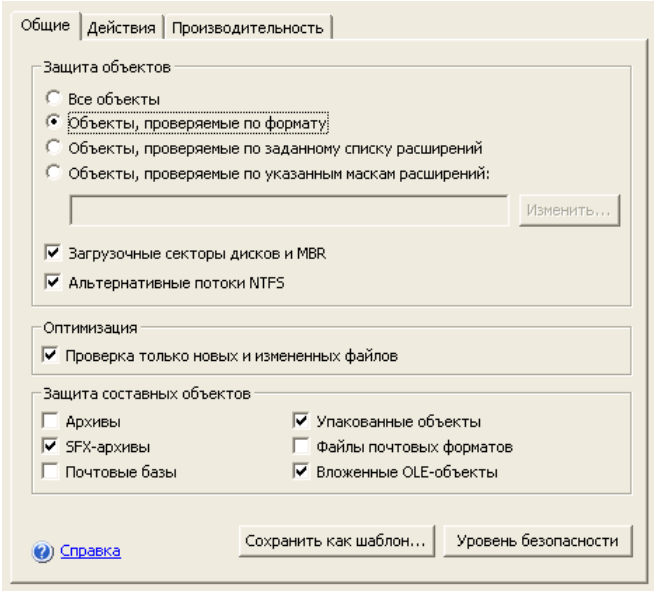

Рисунок 20. Диалоговое окно **Параметры безопасности**, закладка **Общие**

- На закладке **Действия** (см. рис. 21) выполните следующие действия:
  - выберите действие над зараженными объектами (см. п. А.3.5 на стр. 404);
  - выберите действие над подозрительными объектами (см. п. А.3.6 на стр. 407);
  - если требуется, настройте действия над объектами в зависимости от типа обнаруженной в объекте угрозы (см. п. А.3.7 на стр. 409).

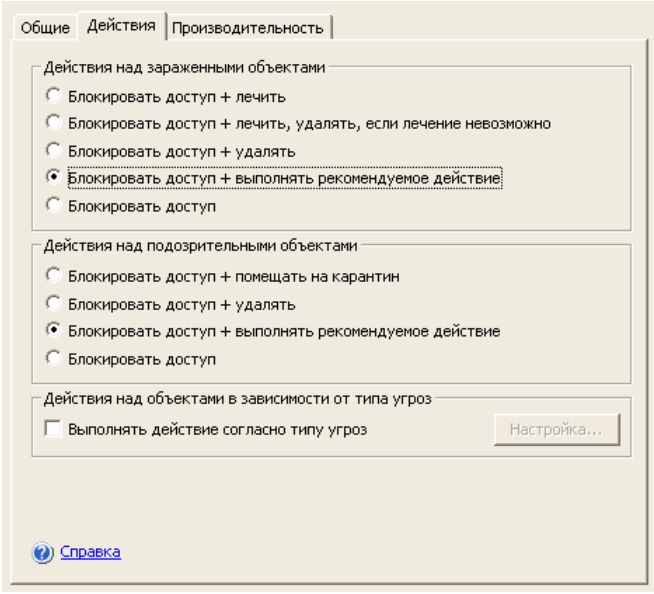

Рисунок 21. Диалоговое окно **Параметры безопасности**, закладка **Действия**

- На закладке **Производительность** (см. рис. 22), если требуется, выполните следующие действия:
  - исключите из обработки файлы по имени или маске (см. п. A.3.8 на стр. 411);
  - исключите из обработки угрозы по названиям или маскам названий (см. п. A.3.9 на стр. 412);
  - укажите максимальную продолжительность проверки объекта (см. п. A.3.10 на стр. 414);
  - укажите максимальный размер проверяемого составного объекта (см. п. A.3.11 на стр. 415);
  - включите или выключите применение технологии iChecker (см. п. A.3.12 на стр. 416);
  - включите или выключите применение технологии iSwift (см. п. A.3.13 на стр. 417).

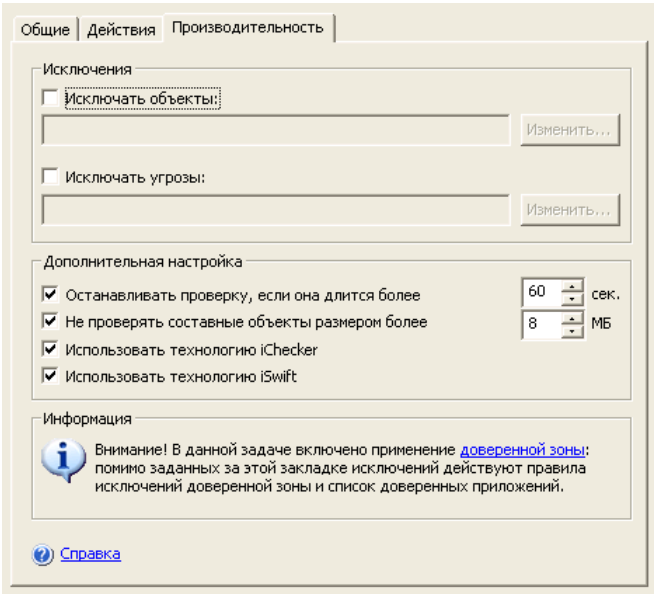

Рисунок 22. Диалоговое окно **Параметры безопасности**, закладка **Производительность**

5. После того как вы настроите нужные параметры безопасности, откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

6.2.2.3. Работа с шаблонами в задаче *Постоянная защита файлов*

В этом разделе содержится следующая информация:

- сохранение набора параметров безопасности в шаблон (см. п. 6.2.2.3.1 на стр. 86);
- просмотр параметров безопасности в шаблоне (см. п. 6.2.2.3.2 на стр. 87);
- применение шаблона (см. п. 6.2.2.3.3 на стр. 88);
- удаление шаблона (см. п. 6.2.2.3.4 на стр. 89).

6.2.2.3.1. Сохранение набора параметров безопасности в шаблон

В задаче **Постоянная защита файлов**, после того как вы настроили параметры безопасности какого-либо из узлов в дереве файловых ресурсов сервера, вы можете сохранить их значения в шаблон, чтобы потом применить этот шаблон для любого другого узла.

Чтобы сохранить набор значений параметров безопасности в шаблон:

1. В дереве консоли разверните узел **Постоянная защита** и выберите вложенный узел **Постоянная защита файлов**.
2. В панели результатов, в дереве файловых ресурсов сервера, выберите узел, значения параметров безопасности которого вы хотите сохранить.
3. Нажмите на кнопку **Настройка** в нижней части диалогового окна.
4. В диалоговом окне **Параметры области защиты**, на закладке **Общие**, нажмите на кнопку **Сохранить в шаблон**.
5. В диалоговом окне **Свойства шаблона** (см. рис. 23) выполните следующие действия:
   - В поле **Имя шаблона** введите название шаблона.
   - В поле **Описание** введите любую дополнительную информацию о шаблоне.

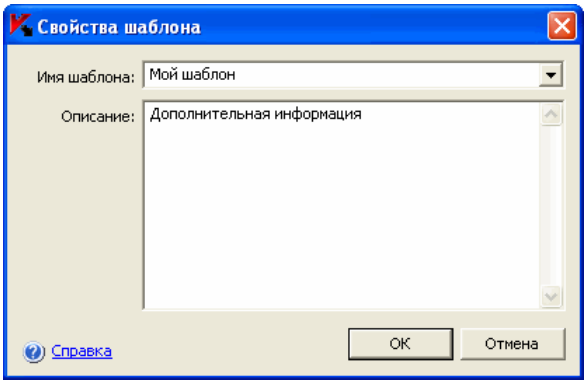

Рисунок 23. Диалоговое окно **Свойства шаблона**

6. Нажмите на кнопку **ОК**. Шаблон с набором значений параметров безопасности будет сохранен.

6.2.2.3.2. Просмотр параметров безопасности в шаблоне

Чтобы просмотреть значения параметров безопасности в созданном шаблоне:

1. В дереве консоли разверните узел **Постоянная защита**.
2. Откройте контекстное меню на задаче **Постоянная защита файлов** и выберите команду **Шаблоны** (см. рис. 24).

Рисунок 24. Диалоговое окно **Шаблоны**

В диалоговом окне **Шаблоны** отображается список шаблонов, которые вы можете применить в задаче **Постоянная защита файлов**.

3. Чтобы просмотреть информацию о шаблоне и значения параметров безопасности, выберите нужный шаблон в списке и нажмите на кнопку **Просмотреть** (см. рис. 25).

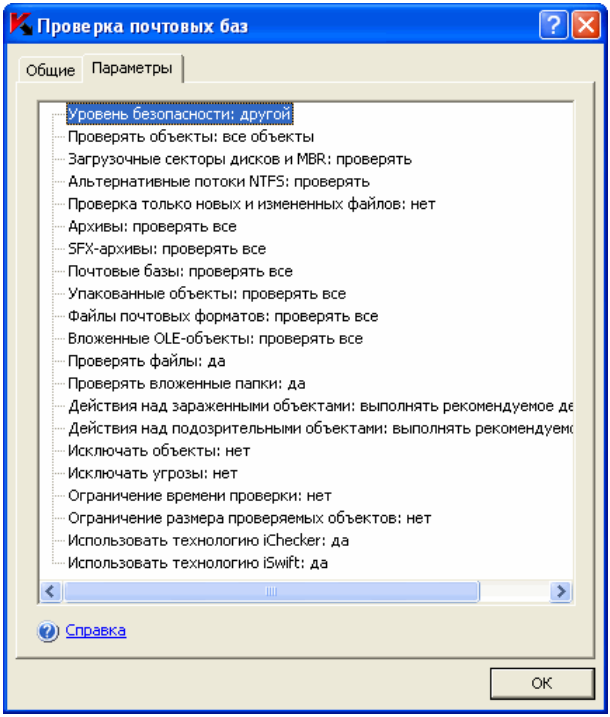

Рисунок 25. Диалоговое окно **<Имя шаблона>**, закладка **Параметры**

На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне; на закладке **Параметры** приводится список значений параметров безопасности, сохраненных в шаблоне.

6.2.2.3.3. Применение шаблона

Чтобы применить шаблон с набором значений параметров безопасности для выбранного узла:

1. Предварительно сохраните набор значений параметров безопасности в шаблон (см. инструкцию в п. 6.2.2.3.1 на стр. 86).
2. В дереве консоли разверните узел **Постоянная защита** и выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов, в дереве файловых ресурсов сервера, откройте контекстное меню на узле, для которого вы хотите применить шаблон, выберите команду **Применить шаблон**.

4. В диалоговом окне **Шаблоны** выберите шаблон, который вы хотите применить.
5. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

Примечание

Если вы примените шаблон к родительскому узлу, то параметры безопасности из шаблона применятся и ко всем вложенным узлам, кроме тех узлов, для которых вы настраивали параметры безопасности отдельно.

Чтобы установить параметры безопасности из шаблона ко всем вложенным узлам, перед применением шаблона снимите флажок с родительского узла в дереве файловых ресурсов сервера, а затем снова установите его. Примените шаблон к родительскому узлу. Все вложенные узлы будут иметь такие же параметры безопасности, как и родительский узел.

6.2.2.3.4. Удаление шаблона

Чтобы удалить шаблон:

1. В дереве консоли разверните узел **Постоянная защита**.
2. Откройте контекстное меню на задаче **Постоянная защита файлов** и выберите команду **Шаблоны** (см. рис. 24).
3. В диалоговом окне **Шаблоны** в списке шаблонов выберите шаблон, который вы хотите удалить, и нажмите на кнопку **Удалить**.
4. В диалоговом окне подтверждения нажмите на кнопку **Да**. Выбранный шаблон будет удален.

6.2.3. Выбор режима защиты объектов

Вы можете выбрать режим защиты объектов в задаче **Постоянная защита файлов**. Подробнее о параметре **Режим защиты объектов** читайте в п. A.3.1 на стр. 399.

Чтобы выбрать режим защиты объектов:

1. В дереве консоли разверните узел **Постоянная защита**.
2. Откройте контекстное меню на задаче **Постоянная защита файлов** и выберите команду **Свойства**.
3. В диалоговом окне **Свойства** на закладке **Общие** (см. рис. 26) выберите режим защиты объектов, который вы хотите установить, и нажмите на кнопку **ОК**.

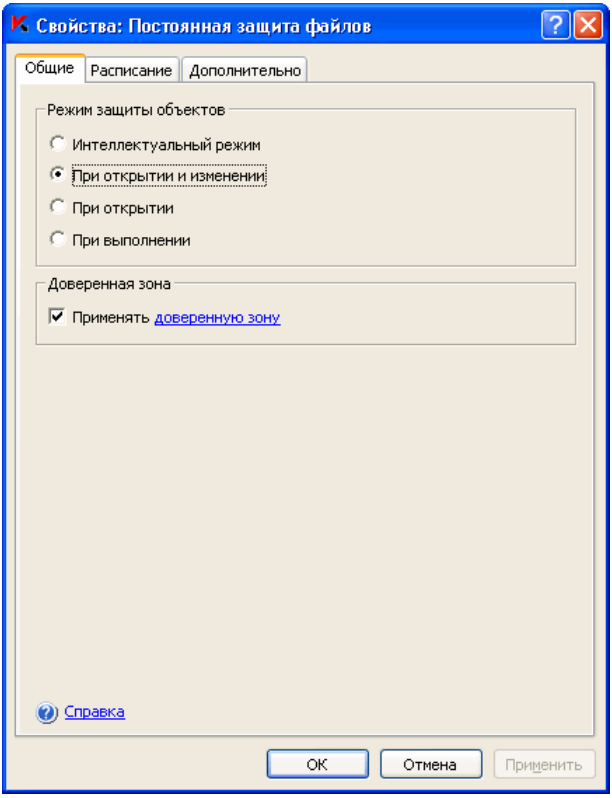

Рисунок 26. Диалоговое окно **Свойства задачи**, закладка **Общие**

6.3. Статистика задачи *Постоянная защита файлов*

Пока выполняется задача **Постоянная защита файлов**, вы можете просматривать в реальном времени информацию о количестве объектов, которые Антивирус обработал с момента ее запуска по текущий момент – *статистику задачи*.

*Чтобы просмотреть статистику задачи **Постоянная защита файлов**:*

1. В дереве консоли разверните узел **Постоянная защита**.
2. Откройте контекстное меню на задаче **Постоянная защита файлов** и выберите команду **Просмотреть статистику**.

В диалоговом окне **Статус задачи** отображается следующая информация об объектах, которые Антивирус обработал с момента запуска задачи по текущий момент.

Поле	Описание
Обнаружено угроз	Количество обнаруженных угроз; например, если Антивирус обнаружит в пяти объектах одну вредоносную программу, значение в этом поле увеличится на единицу.
Обнаружено зараженных объектов	Общее количество обнаруженных зараженных объектов.
Обнаружено подозрительных объектов	Общее количество обнаруженных подозрительных объектов.
Не вылечено объектов	Количество объектов, которые Антивирус не вылечил, так как: а) тип угрозы в объекте не предполагает его лечения; б) объекты этого типа не могут быть вылечены; в) при лечении возникла ошибка.
Объектов, не помещенных на карантин	Количество объектов, которые Антивирус должен был поместить на карантин, но ему это не удалось из-за ошибки, например, из-за отсутствия свободного места на диске.
Не удалено объектов	Количество объектов, которые Антивирус пытался удалить, но ему это не удалось: например, доступ к объекту был заблокирован другой программой.
Не проверено объектов	Количество объектов в области защиты, которые Антивирусу не удалось проверить, так как, например, доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых Антивирус должен был сохранить в резервном хранилище, но это ему не удалось из-за ошибки.
Ошибок проверки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые Антивирус вылечил.

Помещено на карантин	Количество объектов, которые Антивирус поместил на карантин.
Помещено в резервное хранилище	Количество файлов, копии которых Антивирус сохранил в резервном хранилище.
Удалено объектов	Количество объектов, которые Антивирус удалил.
Защищенных паролем объектов	Количество объектов (например, архивов), которые Антивирус пропустил, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, пропущенных Антивирусом, так как их формат искажен.
Проверено объектов	Общее количество объектов, которые Антивирус проверил.

6.4. Настройка задачи *Проверка скриптов*

По умолчанию системная задача **Проверка скриптов** имеет параметры, описанные в таблице 4. Вы можете изменять значения этих параметров – настраивать задачу.

Таблица 4. Параметры задачи *Проверка скриптов* по умолчанию

Параметр	Значение по умолчанию	Описание
Выполнение зараженных скриптов	Запрещено	Антивирус всегда запрещает выполнение скриптов, которые он признает зараженными.
Выполнение подозрительных скриптов	Запрещено	Вы можете указывать действия, которые Антивирус будет выполнит над скриптами, которые он признает подозрительными: запрещать или разрешать их выполнение.

Параметр	Значение по умолчанию	Описание
Доверенная зона	Применяется Список исключений пуст	Единый список исключений, который вы можете применять в задаче **Проверка скриптов**. Глава 8 на стр. 108 содержит информацию о создании и применении доверенной зоны.

*Чтобы настроить задачу **Проверка скриптов**:*

1. В дереве консоли разверните узел **Постоянная защита**.
2. Откройте контекстное меню на задаче **Проверка скриптов** и выберите команду **Свойства**.

   Откроется диалоговое окно **Свойства: Проверка скриптов**.
3. В группе параметров **Действия над подозрительными скриптами** разрешите или запретите выполнение подозрительных скриптов:
   - чтобы разрешить выполнение подозрительных скриптов, выберите **Разрешать выполнение**;
   - чтобы запретить выполнение подозрительных скриптов, выберите **Блокировать выполнение**.
4. В группе параметров **Доверенная зона** включите или отключите применение доверенной зоны:
   - чтобы включить применение доверенной зоны, установите флажок **Применять доверенную зону**;
   - чтобы отключить применение доверенной зоны, снимите флажок **Применять доверенную зону**.

     О том, как добавлять скрипты в список исключений доверенной зоны, читайте в п. 8.2.3 на стр. 114.
5. В диалоговом окне **Свойства: Проверка скриптов** нажмите на кнопку **ОК**, чтобы сохранить изменения.

6.5. Статистика задачи *Проверка скриптов*

Пока задача **Проверка скриптов** выполняется, вы можете просматривать в реальном времени информацию о количестве скриптов, которые Антивирус обработал с момента запуска задачи по текущий момент – *статистику задачи*.

Чтобы просмотреть статистику задачи:

1. В дереве консоли разверните узел **Постоянная защита**.
2. Откройте контекстное меню на задаче **Проверка скриптов** и выберите команду **Просмотреть статистику**.

В диалоговом окне **Статус выполнения задачи** отображается следующая информация:

Поле	Описание
Заблокированно скриптов	Количество скриптов, выполнение которых Антивирус запретил
Опасных скриптов	Количество обнаруженных опасных скриптов
Подозрительных скриптов	Количество обнаруженных подозрительных скриптов
Обработано скриптов	Общее количество обработанных скриптов

ГЛАВА 7. БЛОКИРОВАНИЕ ДОСТУПА С КОМПЬЮТЕРОВ В ЗАДАЧЕ ПОСТОЯННАЯ ЗАЩИТА ФАЙЛОВ

В этой главе содержится следующая информация:

7.1. О блокировании доступа с компьютеров к защищаемому серверу

Когда выполняется задача **Постоянная защита файлов**, вы можете временно блокировать доступ с зараженных компьютеров к защищаемому серверу.

Вы можете блокировать доступ с компьютеров двумя способами:

- **включить автоматическое блокирование доступа с компьютеров**. Как только какой-либо компьютер в сети попытается записать на защищаемый сервер зараженный или подозрительный объект, Антивирус признает этот компьютер *зараженным* и выполнит указанные вами действия: временно заблокирует доступ с компьютера к файлам на сервере и / или запустит указанный вами исполняемый файл. По умолчанию автоматическое блокирование доступа с компьютеров выключено;
- **вручную блокировать доступ с зараженных компьютеров**. Если у вас есть информация о том, что какой-либо компьютер в локальной сети заражен, вы можете вручную заблокировать доступ с него к защищаемому серверу: добавить компьютер в список блокирования и указать время, в течение которого ему будут недоступны объекты на защищаемом сервере.

Вы можете в любой момент разблокировать доступ с компьютера к серверу.

Все операции по блокированию или разблокированию доступа с компьютеров регистрируются в журнале системного аудита.

Список заблокированных компьютеров автоматически сохраняется между сеансами работы Антивируса.

7.2. Включение или отключение автоматического блокирования доступа с компьютеров

Чтобы включить или выключить функцию блокирования доступа с компьютеров:

1. В дереве консоли разверните узел **Постоянная защита**, а затем узел **Постоянная защита файлов**, чтобы отобразить вложенный узел **Блокирование доступа с компьютеров**.
2. Выполните одно из следующих действий:
   - чтобы включить автоматическое блокирование доступа с компьютеров к серверу, откройте контекстное меню на узле **Блокирование доступа с компьютеров** и выберите команду **Включить блокирование доступа с компьютеров**.
   - чтобы отключить автоматическое блокирование доступа с компьютеров к серверу, откройте контекстное меню на узле **Блокирование доступа с компьютеров** и выберите команду **Отключить блокирование доступа с компьютеров**.
3. Нажмите на кнопку **ОК**.

Примечание

Если вы включите функцию автоматического блокирования доступа с компьютеров, она будет выполняться только тогда, когда выполняется задача **Постоянная защита файлов**.

Как только вы отключите функцию автоматического блокирования, все компьютеры в списке блокирования получат доступ к файлам на сервере.

7.3. Настройка параметров автоматического блокирования доступа с компьютеров

В этом разделе описано, как включить и настроить автоматическое блокирование доступа с компьютеров к серверу. Описание параметров блокирования приводится в п. A.4 на стр. 418.

Чтобы настроить параметры автоматического блокирования доступа с компьютеров:

1. В дереве консоли разверните узел **Постоянная защита**, а затем узел **Постоянная защита файлов**, чтобы отобразить вложенный узел **Блокирование доступа с компьютеров**.
2. Откройте контекстное меню на узле **Блокирование доступа с компьютеров** и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: Блокирование доступа с компьютеров** на закладке **Общие** убедитесь, что флажок **Включить блокирование доступа с компьютеров к серверу** установлен (см. рис. 27).
4. В группе параметров **Действия над компьютером** установите флажки рядом с действиями, которые Антивирус выполнит при попытке записи с компьютера на сервер зараженного или подозрительного объекта (см. п. A.4.2 на стр. 420).
5. Если вы выбрали **Блокировать доступ с компьютера к серверу**, то задайте промежуток времени, на который вы хотите заблокировать доступ к серверу с компьютеров, в днях, часах или минутах;
6. Если вы выбрали **Запускать исполняемый файл**, то нажмите на кнопку списка 

и в диалоговом окне **Исполняемый файл** (см. рис. 28) укажите исполняемый файл (имя и полный путь к нему), а также учетную запись, с правами которой исполняемый файл будет выполнен.

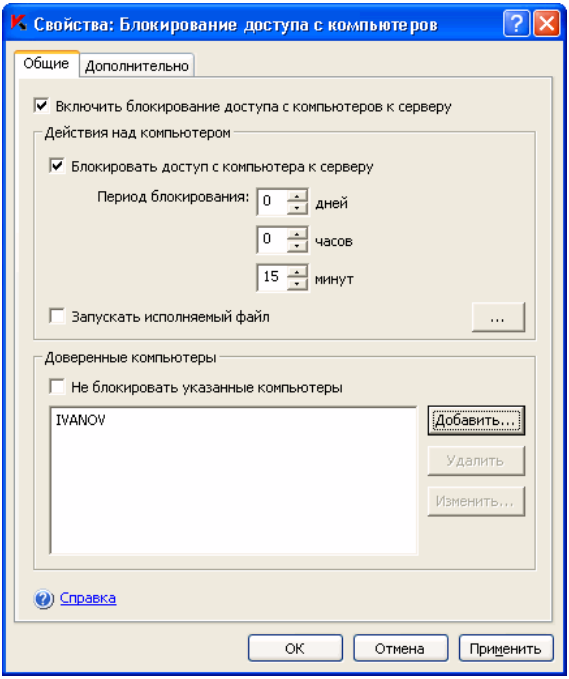

Рисунок 27. Диалоговое окно **Свойства: Блокирование доступа с компьютеров**, закладка **Общие**

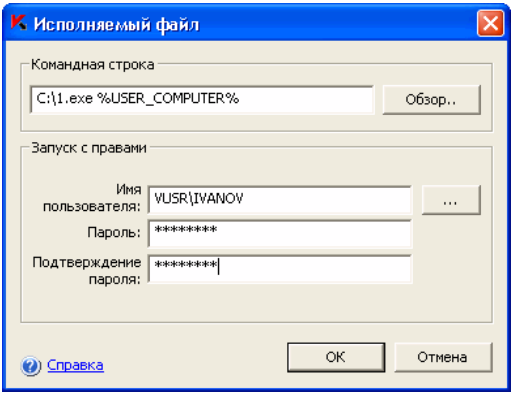

Рисунок 28. Диалоговое окно **Исполняемый файл**

7. Нажмите на кнопку **ОК**.

7.4. Исключение компьютеров из автоматического блокирования (Доверенные компьютеры)

Вы можете сформировать список доверенных компьютеров (подробнее о параметре читайте в п. A.4.3 на стр. 421).

Чтобы добавить компьютер в список доверенных:

1. В дереве консоли разверните узел **Постоянная защита**, а затем узел **Постоянная защита файлов**, чтобы отобразить вложенный узел **Блокирование доступа с компьютеров**.
2. Откройте контекстное меню на узле **Блокирование доступа с компьютеров** и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: Блокирование доступа с компьютеров** на закладке **Общие** (см. рис. 27) убедитесь, что флажок **Включить блокирование доступа с компьютеров к серверу** установлен (см. п. A.4.1 на стр. 419).
4. В группе параметров **Доверенные компьютеры** установите флажок **Не блокировать указанные компьютеры** и выполните следующие действия:

   а) Нажмите на кнопку **Добавить**. Откроется диалоговое окно **Добавление компьютера** (см. рис. 29).

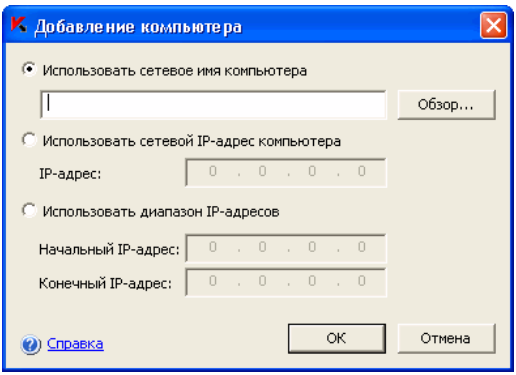

Рисунок 29. Диалоговое окно **Добавление компьютера**

б) Укажите сетевое имя или IP-адрес компьютера:

- выберите **Использовать сетевое имя компьютера** и укажите NetBIOS-имя компьютера в сети;
- укажите статический IP-адрес: выберите **Использовать сетевой IP-адрес компьютера** и введите IP-адрес компьютера;
- укажите диапазон IP-адресов: выберите **Использовать диапазон IP-адресов**, введите первый IP-адрес диапазона в поле **Начальный IP-адрес**, а последний IP-адрес в поле **Конечный IP-адрес**. Все компьютеры, IP-адреса которых входят в указанный диапазон, будут считаться доверенными.

в) Нажмите на кнопку **ОК**.

5. Нажмите на кнопку **ОК** в диалоговом окне **Свойства**.

7.5. Предотвращение вирусных эпидемий

В этом разделе описано, как включить или выключить предотвращение вирусных эпидемий. Описание функции *Предотвращение вирусных эпидемий* приводится в п. A.4.4 на стр. 422.

Чтобы включить / выключить предотвращение вирусных эпидемий:

1. В дереве консоли разверните узел **Постоянная защита**, а затем узел **Постоянная защита файлов**, чтобы отобразить вложенный узел **Блокирование доступа с компьютеров**.
2. Откройте контекстное меню на узле **Блокирование доступа с компьютеров** и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: Блокирование доступа с компьютеров** откройте закладку **Дополнительно** (см. рис. 30).

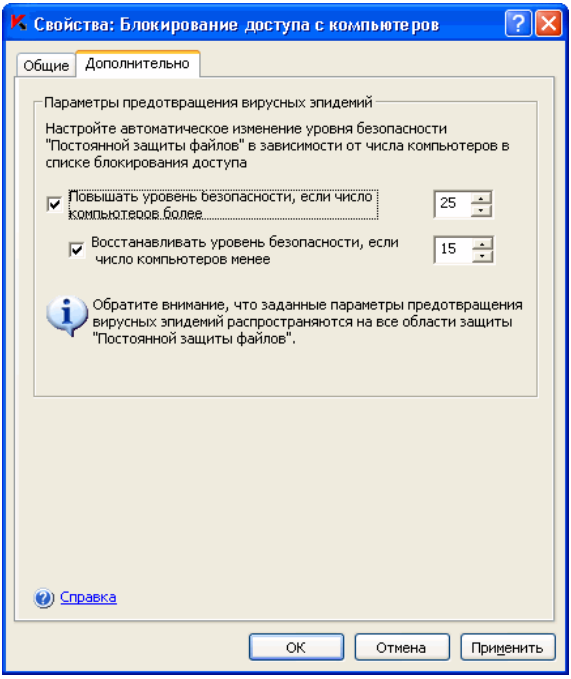

Рисунок 30. Диалоговое окно **Свойства: Блокирование доступа с компьютеров**, закладка **Дополнительно**

4. На закладке **Дополнительно** выполните одно из следующих действий:

   - Чтобы включить предотвращение вирусных эпидемий:

     а) установите флажок **Повышать уровень безопасности, если число компьютеров более**;

     б) укажите количество компьютеров с заблокированным доступом, по достижению которого Антивирус повысит уровень безопасности.

     в) Если требуется, включите восстановление уровня безопасности, когда количество компьютеров с заблокированным доступом снизится до указанного в поле **Восстанавливать уровень безопасности, если число компьютеров менее**.

- Чтобы выключить предотвращение вирусных эпидемий, снимите флажок **Повышать уровень безопасности, если число компьютеров более**.

5. Нажмите на кнопку **ОК**.

7.6. Просмотр списка компьютеров, с которых запрещен доступ к серверу

Внимание!

Компьютерам в списке блокирования доступа к серверу запрещен доступ к защищаемому серверу только тогда, когда выполняется задача **Постоянная защита файлов** и включена функция автоматического блокирования доступа с компьютеров.

Чтобы просмотреть список компьютеров, которым в текущий момент запрещен доступ к защищаемому серверу:

1. В дереве консоли разверните узел **Постоянная защита**, а затем узел **Постоянная защита файлов**.

2. Откройте вложенный узел **Блокирование доступа с компьютеров** (см. рис. 31).

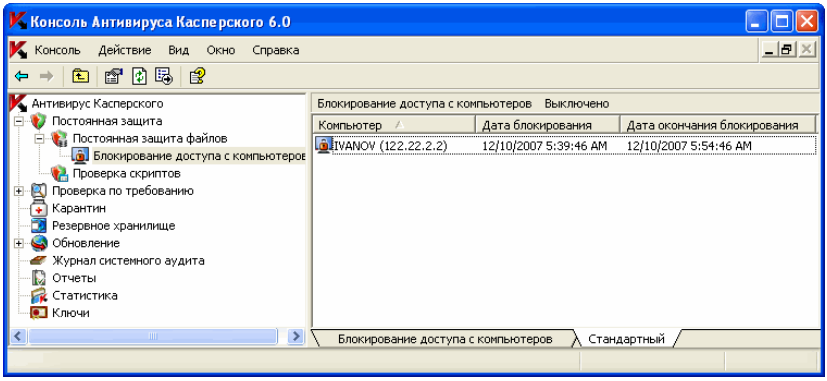

Рисунок 31. Окно **Блокирование доступа с компьютеров**

В панели результатов отображается следующая информация о компьютерах, с которых запрещен доступ к серверу:

Поле	Описание
Имя компьютера	Информация о компьютере в списке блокирования, полученная Антивирусом (сетевое имя, IP-адрес компьютера)
Дата блокирования	Дата и время, когда доступ с компьютера был заблокирован, в формате, заданном региональными настройками Microsoft Windows компьютера, на котором установлена консоль Антивируса
Дата окончания блокирования	Дата и время, когда доступ с компьютера будет разблокирован, в формате, заданном региональными настройками Microsoft Windows компьютера, на котором установлена консоль Антивируса

7.7. Блокирование доступа с компьютеров вручную

Если у вас есть информация о том, что какой-либо компьютер в локальной сети заражен, вы можете вручную временно заблокировать доступ с него к защищаемому серверу.

Внимание!

Компьютерам в списке блокирования доступа запрещен доступ к защищаемому серверу только тогда, когда выполняется задача **Постоянная защита файлов** и включено автоматическое блокирование доступа с компьютеров.

Чтобы вручную заблокировать доступ с компьютера к серверу:

1. В дереве консоли разверните узел **Постоянная защита**, а затем узел **Постоянная защита файлов**.
2. Убедитесь, что включено автоматическое блокирование доступа с компьютеров (см. п. 7.2 на стр. 97).
3. Откройте контекстное меню на вложенном узле **Блокирование доступа с компьютеров** и выберите **Добавить в список блокирования**.
4. В диалоговом окне **Добавление компьютера в список блокирования** (см. рис. 32) укажите сетевое имя компьютера, доступ с которого к серверу вы хотите заблокировать.

Примечание

В поле **Имя компьютера** указывайте только сетевые NetBIOS-имена компьютеров; не указывайте DNS-адреса.

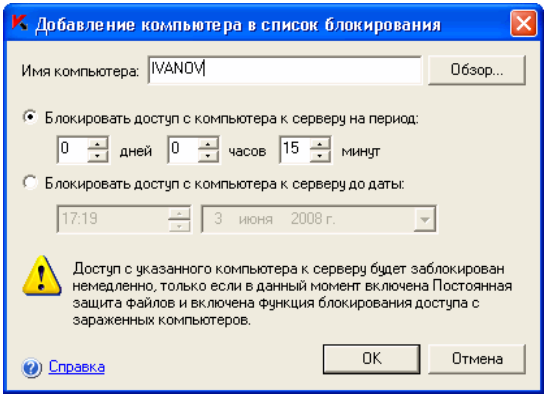

Рисунок 32. Диалоговое окно **Добавление компьютера в список блокирования**

5. Выполните одно из следующих действий:

   - выберите **Блокировать доступ с компьютера к серверу на период** и укажите промежуток времени, в течение которого доступ с компьютера к серверу будет запрещен;
   - выберите **Блокировать доступ с компьютера к серверу до даты** и укажите дату и время, когда компьютер будет разблокирован.

6. Нажмите на кнопку **ОК**.

7.8. Разблокирование доступа с компьютеров

Вы можете в любой момент разблокировать доступ с компьютера к защищаемому серверу.

Чтобы разблокировать доступ с компьютера:

1. В дереве консоли разверните узел **Постоянная защита**, а затем узел **Постоянная защита файлов**.

2. Выберите вложенный узел **Блокирование доступа с компьютеров**.
3. В окне **Блокирование доступа с компьютеров**, в списке заблокированных компьютеров, откройте контекстное меню на строке с информацией о компьютере, который вы хотите разблокировать, и выберите команду **Разрешить доступ с компьютера**.

7.9. Просмотр статистики блокирования

Вы можете просматривать информацию о количестве компьютеров, доступ с которых к защищаемому серверу был заблокирован с момента последнего запуска Антивируса – *статистику блокирования*.

Чтобы просмотреть статистику блокирования:

1. В дереве консоли разверните узел **Постоянная защита**.
2. Разверните узел **Постоянная защита файлов**.
3. Откройте контекстное меню на узле **Блокирование доступа с компьютеров** и выберите команду **Просмотреть статистику** (см. рис. 33).

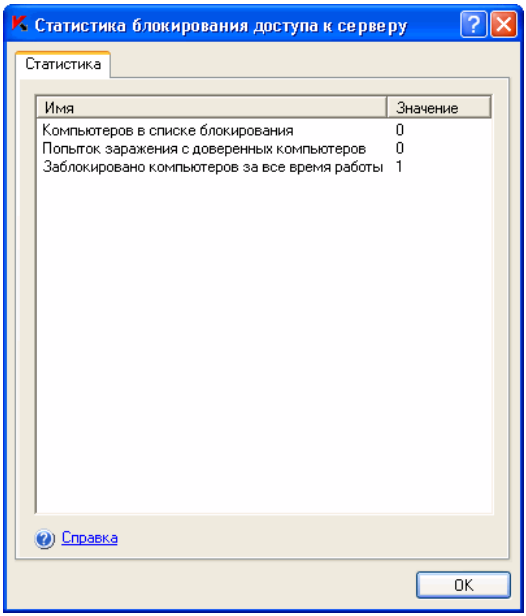

Рисунок 33. Диалоговое окно **Статистика блокирования доступа к серверу**

В диалоговом окне **Статистика блокирования доступа к серверу** отображается следующая информация:

Поле	Описание
Компьютеров в списке блокирования	Количество компьютеров в списке блокирования доступа в текущий момент
Попыток заражения с доверенных компьютеров	Количество попыток записи на сервер зараженных или подозрительных объектов с доверенных компьютеров с момента включения функции автоматического блокирования
Заблокировано компьютеров за все время работы	Общее количество компьютеров, добавленных в список блокирования автоматически при попытке записи на сервер зараженных или подозрительных объектов с момента включения функции автоматического блокирования

ГЛАВА 8. ДОВЕРЕННАЯ ЗОНА

В этой главе содержится следующая информация:

- о доверенной зоне Антивируса (см. п. 8.1 на стр. 108);
- добавление исключений в доверенную зону (см. 8.2 на стр. 110);
- применение доверенной зоны (см. п. 8.3 на стр. 119).

8.1. О доверенной зоне Антивируса

Вы можете сформировать единый список исключений из области защиты (проверки) и, когда потребуется, применять эти исключения в выбранных задачах проверки по требованию и задаче **Постоянная защита файлов**. Этот список исключений называется *доверенной зоной*.

В доверенной зоне Антивируса могут находиться следующие объекты:

- файлы, к которым обращаются процессы приложений, чувствительных к файловым перехватам (*доверенные процессы*);
- файлы, доступ к которым выполняется в операциях резервного копирования (*операции резервного копирования*);
- объекты, указанные пользователем по их местоположению и/или угрозе в них (*правила исключений*).

По умолчанию доверенная зона применяется в задачах **Постоянная защита файлов** и **Проверка скриптов**; системных и вновь созданных пользовательских задачах проверки по требованию.

Доверенные процессы (применяется только в задаче **Постоянная защита файлов**)

Некоторые приложения на сервере могут работать нестабильно, если файлы, к которым они обращаются, перехватываются антивирусным приложением. К таким приложениям относятся, например, системные приложения домен-контроллеров.

Чтобы не нарушать стабильную работу таких приложений, вы можете отключить постоянную защиту файлов, к которым обращаются выполняющиеся процессы этих приложений – сформировать в доверенной зоне список доверенных процессов.

Корпорация Майкрософт рекомендует исключать из постоянной защиты файлы некоторых таких приложений как неподверженные заражению. Вы можете просмотреть список файлов, рекомендуемых к исключению, на веб-сайте корпорации Майкрософт http://www.microsoft.com/rus/, код статьи: KB822158.

Вы можете применять доверенную зону с включением функции *Доверенные процессы* или не включая ее.

Обратите внимание, что если исполняемый файл процесса изменяется, например, обновляется, то Антивирус исключает его из списка доверенных.

Операции резервного копирования (применяется только в задаче **Постоянная защита файлов**)

На время резервного копирования файлов вы можете отключать постоянную защиту файлов, доступ к которым выполняется в операциях резервного копирования. Антивирус не проверяет файлы, которые приложение резервного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

Вы можете применять доверенную зону с отключением постоянной защиты файлов на время резервного копирования или без него.

Правила исключений (применяется в задачах **Постоянная защита файлов** и **Проверка скриптов** и задачах проверки по требованию)

Вы можете исключать объекты из проверки в отдельных задачах, не используя доверенную зону, или вы можете сохранить единый список исключений в доверенной зоне и когда потребуется, применять эти исключения в выбранных задачах: **Постоянная защита файлов**, **Проверка скриптов** или задачах проверки по требованию.

Вы можете добавлять в доверенную зону объекты по их местоположению на сервере, по названию обнаруженной в них угрозы или совмещать эти признаки.

Добавляя в доверенную зону новое исключение, вы задаете для него правило (признаки, по которым Антивирус будет пропускать объекты), и указываете, на какие задачи (**Постоянная защита файлов**, **Проверка скриптов** и/или **Проверка по требованию**) это правило распространяется.

Согласно заданному вами правилу, Антивирус может пропускать в задачах указанных компонентов:

- указанные угрозы в указанных областях сервера;
- все угрозы в указанных областях сервера;

- указанные угрозы во всей области проверки.

Если при установке Антивируса вы выбрали **Добавить к исключениям программы удаленного администрирования** и **Добавить к исключениям файлы, рекомендованные Microsoft**, то эти правила исключений применяются в задаче **Постоянная защита файлов**, а также в системных задачах проверки по требованию кроме задач **Проверка объектов на карантине** и **Проверка целостности приложения**.

8.2. Добавление исключений в доверенную зону

В этом разделе содержится следующая информация:

- добавление процессов в список доверенных (см. п. 8.2.1 на стр. 110);
- отключение постоянной защиты файлов на время резервного копирования (см. п. 8.2.2 на стр. 113);
- добавление правил исключений (см. п. 8.2.3 на стр. 114).

8.2.1. Добавление процессов в список доверенных

Чтобы не нарушать стабильную работу приложений, чувствительных к файловым перехватам, вы можете отключить постоянную защиту файлов, к которым обращаются выполняющиеся процессы этих приложений – сформировать в доверенной зоне список доверенных процессов.

Вы можете добавить процесс в список доверенных одним из следующих способов:

- выбрать процесс из списка процессов, выполняемых на защищаемом сервере в текущий момент;
- выбрать исполняемый файл процесса независимо от того, выполняется ли процесс в текущий момент.

Примечание

Если исполняемый файл процесса изменяется, Антивирус исключает этот процесс из списка доверенных.

Чтобы добавить процесс в список доверенных:

1. В консоли Антивируса в ММС откройте контекстное меню на названии оснастки Антивируса и выберите команду **Настроить доверенную зону**.
2. В диалоговом окне **Доверенная зона** на закладке **Доверенные процессы** (см. рис. 34) включите функцию *Доверенные процессы*: установите флажок **Не проверять файловую активность указанных процессов**.

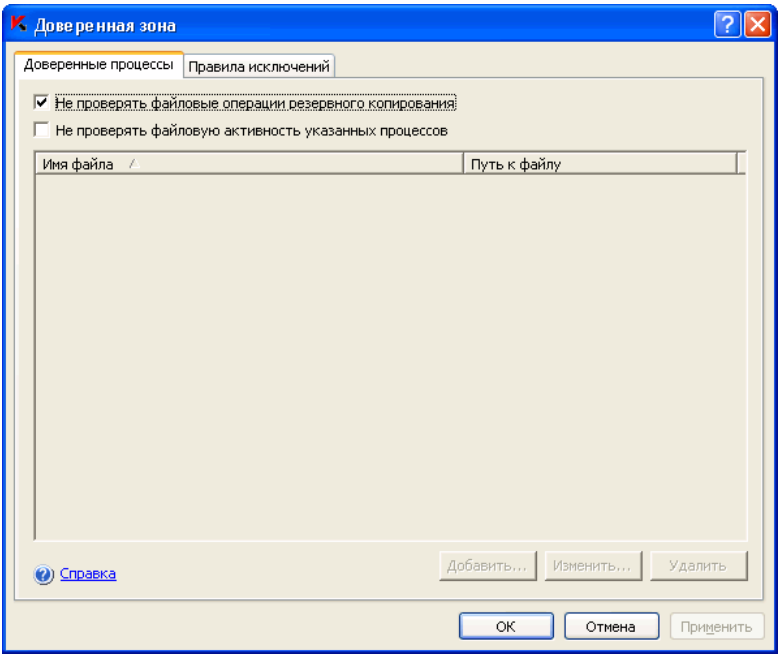

Рисунок 34. Диалоговое окно **Доверенная зона**, закладка **Доверенные процессы**

3. Добавьте доверенный процесс из списка выполняемых процессов или укажите исполняемый файл процесса.
   - Чтобы добавить процесс из списка выполняемых процессов:
     а) Нажмите на кнопку **Добавить**.
     б) В диалоговом окне **Добавление доверенного процесса** (см. рис. 35) нажмите на кнопку **Процессы**.

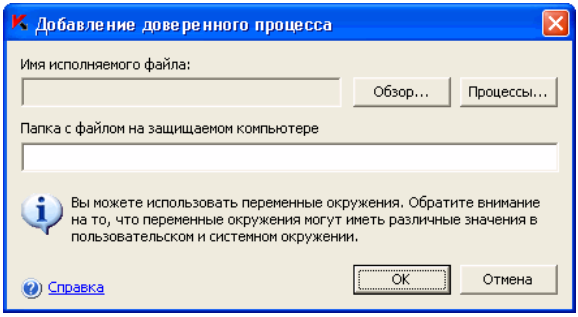

Рисунок 35. Диалоговое окно **Добавление доверенного процесса**

в) В диалоговом окне **Активные процессы** (см. рис. 36) выберите нужный процесс и нажмите на кнопку **OK**.

Чтобы найти нужный процесс в списке, вы можете отсортировать процессы по имени, PID или пути к исполняемому файлу процесса.

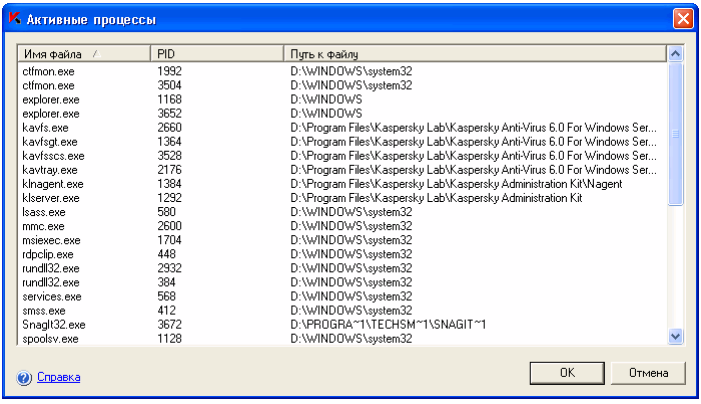

Рисунок 36. Диалоговое окно **Активные процессы**

> **Примечание**
>
> Вы должны входить в группу локальных администраторов на защищаемом сервере, чтобы просматривать активные процессы на нем.

Выбранный процесс будет добавлен в список доверенных процессов в диалоговом окне **Доверенные процессы**.

- Чтобы выбрать исполняемый файл процесса на диске защищаемого сервера, выполните следующие действия:

  а) На закладке **Доверенные процессы** нажмите на кнопку **Добавить**.

  б) В диалоговом окне **Добавление доверенного процесса** нажмите на кнопку **Обзор** и выберите исполняемый файл процесса на локальном диске защищаемого сервера. Нажмите на кнопку **ОК**.

  В диалоговом окне **Добавление доверенного процесса** отобразится название файла и путь к нему.

  Указывая пути, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

  Примечание

  Антивирус не считает процесс доверенным, если путь к исполняемому файлу процесса отличается от пути, указанного вами в поле **Путь к файлу**. Если вы хотите, чтобы доверенным считался процесс, запущенный из файла, который может быть расположен в любой папке, то в поле **Путь к файлу** введите символ *.

  в) Нажмите на кнопку **ОК**.

  Имя выбранного исполняемого файла процесса отобразится в списке доверенных процессов на закладке **Доверенные процессы**.

4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
5. Убедитесь, что доверенная зона применяется в задаче **Постоянная защита файлов** (см. п. 8.3 на стр. 119).

8.2.2. Отключение постоянной защиты файлов на время резервного копирования

На время резервного копирования файлов вы можете отключать постоянную защиту файлов, доступ к которым выполняется в операциях резервного копирования. Антивирус не проверяет файлы, которые приложение резерв-

ного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

Примечание

Информация о количестве файлов, которые Антивирус пропускает в операциях резервного копирования, не отображается в диалоговом окне **Статистика** задачи **Постоянная защита файлов**.

Чтобы отключить постоянную защиту файлов на время резервного копирования:

1. В консоли Антивируса в ММС откройте контекстное меню на названии оснастки Антивируса и выберите команду **Настроить доверенную зону**.
2. В диалоговом окне **Доверенная зона**, на закладке **Доверенные процессы** выполните одно из следующих действий:
   - Чтобы отключить постоянную защиту файлов, доступ к которым выполняется в задаче резервного копирования, установите флажок **Не проверять файловые операции резервного копирования**.
   - Чтобы включить постоянную защиту файлов, доступ к которым выполняется в задаче резервного копирования, снимите флажок **Не проверять файловые операции резервного копирования**.
3. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
4. Убедитесь, что доверенная зона применяется в задаче **Постоянная защита файлов** (см. п. 8.3 на стр. 119).

8.2.3. Добавление правил исключений

Чтобы добавить правило исключений:

1. В консоли Антивируса в ММС откройте контекстное меню на названии оснастки Антивируса и выберите команду **Настроить доверенную зону**.
2. В диалоговом окне **Доверенная зона**, на закладке **Правила исключений**, нажмите на кнопку **Добавить**.

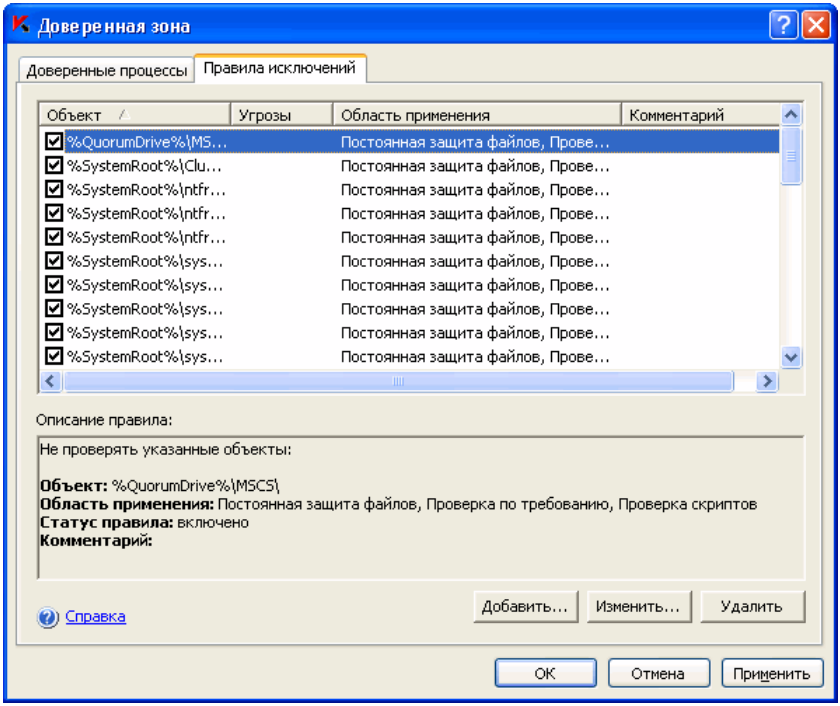

Рисунок 37. Диалоговое окно **Доверенная зона**, закладка **Правила исключений**

Откроется диалоговое окно **Правило исключения**.

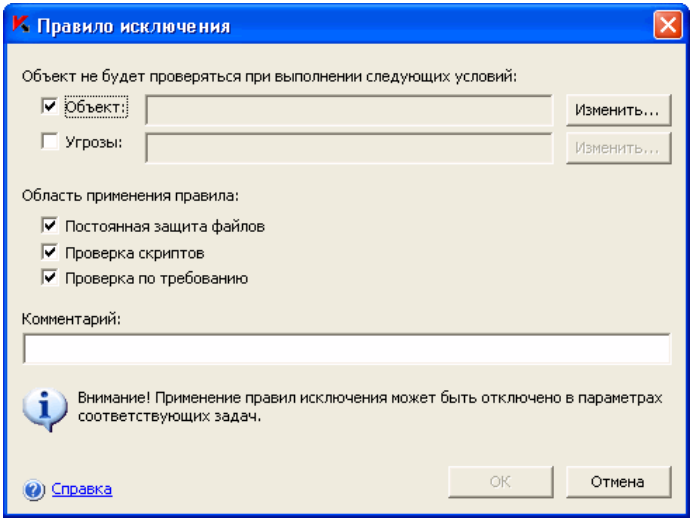

Рисунок 38. Диалоговое окно **Правило исключения**

3. Укажите правило, по которому Антивирус будет исключать объект.

Примечание

Чтобы исключить *указанные угрозы в указанных областях*, установите флажок **Объект** и флажок **Угрозы**.

Чтобы исключить *все угрозы в указанных областях*, установите флажок **Объект**; снимите флажок **Угрозы**.

Чтобы исключить *указанные угрозы во всей области проверки*, снимите флажок **Объект** и установите флажок **Угрозы**.

- *Если вы хотите указать местоположение объекта*, установите флажок **Объект**, нажмите на кнопку **Изменить** и в диалоговом окне **Выбор объекта** (см. рис. 39) укажите объект, который будет исключен из проверки, а затем нажмите на кнопку **ОК**:
  - **Предопределенная область проверки**. Выберите в списке одну из предустановленных областей проверки.
  - **Диск или папка**. Укажите диск сервера или папку на сервере или в локальной сети.
  - **Файл**. Укажите файл на сервере или в локальной сети.

- **Файл или URL-адрес скрипта**. Укажите скрипт на защищаемом сервере, в локальной сети или интернете.

> **Примечание**
>
> Вы можете задавать маски названий объектов, используя символы ? и *.

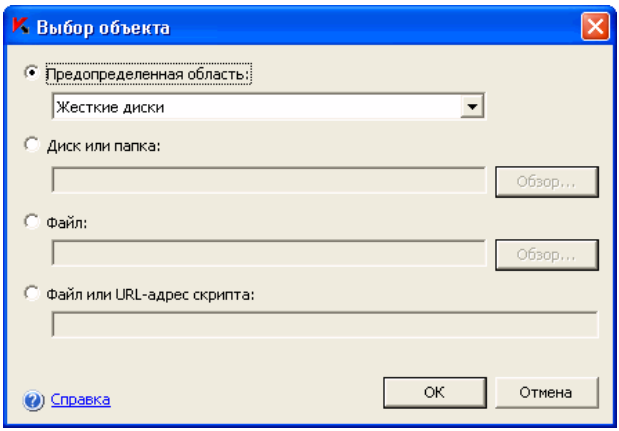

Рисунок 39. Диалоговое окно **Выбор объекта**

- *Если вы хотите указать название угрозы*, нажмите на кнопку **Изменить** и в диалоговом окне **Список исключений** (см. рис. 40) добавьте названия угроз (подробнее о параметре читайте в п. A.3.9 на стр. 412).

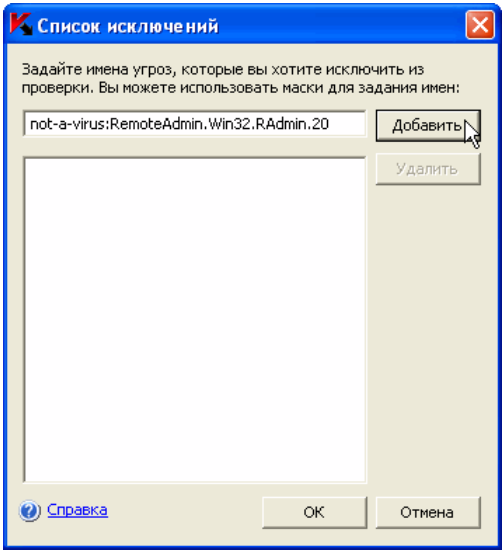

Рисунок 40. Диалоговое окно **Список исключений**

4. В диалоговом окне **Правило исключения** под заголовком **Область применения правила** установите флажки рядом с названиями функциональных компонентов, в задачах которых правило исключения будет применяться.
5. Нажмите **ОК**.

- Чтобы отредактировать правило, в диалоговом окне **Доверенная зона**, на закладке **Правила исключений**, выберите правило, которое вы отредактировать, нажмите на кнопку **Изменить** и выполните изменение в диалоговом окне **Правило исключения**.
- Чтобы удалить правило, в диалоговом окне **Доверенная зона** на закладке **Правила исключений** выберите правило, которое вы хотите удалить, нажмите на кнопку **Удалить** и подтвердите операцию.

6. Нажмите **ОК** в диалоговом окне **Доверенная зона**.

8.3. Применение доверенной зоны

По умолчанию доверенная зона применяется в задачах компонента **Постоянная защита**, системных и вновь созданных задачах проверки по требованию.

Вы можете включать или выключать применение доверенной зоны в отдельных задачах в диалоговом окне **Свойства задачи**.

После того как вы включите или выключите доверенную зону, исключения в ней начнут или перестанут действовать в задачах **Постоянная защита файлов** и **Проверка скриптов** немедленно, а в задачах проверки по требованию – при следующем запуске задачи.

Чтобы применить исключения доверенной зоны в задаче:

1. В консоли ММС откройте контекстное меню на названии задачи и в диалоговом окне **Свойства задачи** на закладке **Общие** установите флажок **Применять доверенную зону**.
2. Нажмите на кнопку **ОК**.

ГЛАВА 9. ПРОВЕРКА ПО ТРЕБОВАНИЮ

В этой главе содержится следующая информация:

- о задачах проверки по требованию (см. п. 9.1 на стр. 120);
- настройка задач проверки по требованию (см. п. 9.2 на стр. 121);
- выполнение задачи проверки по требованию в фоновом режиме (см. п. 9.3 на стр. 143);
- статистика задач проверки по требованию (см. п. 9.4 на стр. 145).

9.1. О задачах проверки по требованию

В Антивирусе предусмотрено четыре системные задачи проверки по требованию:

- Задача **Полная проверка компьютера** по умолчанию выполняется еженедельно по расписанию. Антивирус проверяет все объекты на жестких дисках и съемных носителях защищаемого сервера, применяя параметры безопасности, значения которых соответствуют уровню **Рекомендуемый** (см. п. 9.2.2.1 на стр. 131). Вы можете изменять параметры задачи **Полная проверка компьютера**.
- Задача **Проверка объектов на карантине** по умолчанию выполняется по расписанию после каждого обновления баз. Антивирус проверяет папку карантина с параметрами, перечисленными в п. 11.3 на стр. 175. Вы не можете изменять параметры задачи **Проверка объектов на карантине**.
- Задача **Проверка при старте системы** выполняется каждый раз при старте Антивируса после загрузки операционной системы. Антивирус проверяет объекты автозапуска, собственные программные модули, загрузочные секторы и главные загрузочные записи жестких и съемных дисков, системную память и память процессов. Антивирус применяет предустановленный уровень безопасности **Рекомендуемый** (см. п. 9.2.2.1 на стр. 131). Вы можете изменять расписание задачи или отключить ее запуск по расписанию.

- Задача **Проверка целостности приложения** выполняется по расписанию при запуске Антивируса. Антивирус проверяет подлинность своих исполняемых модулей. Вы не можете изменять параметры задачи **Проверка целостности приложения**. Вы можете изменять параметры расписания или отключить запуск этой задачи по расписанию.

Вы можете создавать *пользовательские задачи проверки по требованию*. Например, вы можете создать задачу проверки папок общего доступа на сервере.

Антивирус может одновременно выполнять несколько задач проверки по требованию.

Подробнее о том, какие категории задач предусмотрены в Антивирусе по месту их создания и выполнения, читайте в п. 5.1 на стр. 54.

Подробнее о функциях *Постоянная защита* и *Проверка по требованию* читайте в п. 1.1.1 на стр. 15.

Глава 5 на стр. 54 содержит информацию о том, как управлять задачами в консоли Антивируса в ММС.

9.2. Настройка задач проверки по требованию

Вы можете настраивать системную задачу **Полная проверка компьютера**, а также пользовательские задачи проверки по требованию.

О том, как создать пользовательскую задачу проверки по требованию, см. п. 5.2 на стр. 56.

Чтобы настроить задачу проверки по требованию:

1. В дереве консоли разверните узел **Проверка по требованию**.
2. Выберите задачу, которую вы хотите настроить, чтобы открыть ее.
3. Настройте параметры задачи: сформируйте область проверки; если требуется, измените параметры безопасности всей области проверки или ее отдельных узлов. По умолчанию системная задача **Полная проверка компьютера**, а также вновь созданные пользовательские задачи имеют параметры, описанные в таблице 5.
4. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

Таблица 5. Параметры по умолчанию задачи **Полная проверка компьютера**

Параметр	Значение	Как настроить
Область проверки	Весь сервер В дереве файловых ресурсов сервера не установлен флажок **Папки общего доступа** – Антивирус проверяет общие папки по их фактическому пути на жестком диске.	Вы можете ограничить область проверки (см. п. 9.2.1 на стр. 123).
Параметры безопасности	Единые для всей области проверки, соответствуют уровню безопасности **Рекомендуемый**	Для выбранных узлов в дереве файловых ресурсов сервера вы можете: • выбрать другой предустановленный уровень безопасности (см. п. 9.2.2.1 на стр. 131); • вручную изменить параметры безопасности (см. п. 9.2.2 на стр. 130). Вы можете сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла (см. п. 9.2.2.3 на стр. 139).

Параметр	Значение	Как настроить
Доверенная зона	Применяется Исключаются программы удаленного администрирования **RemoteAdmin** и файлы, рекомендованные корпорацией Microsoft, если при установке Антивируса вы выбрали **Добавить к исключениям угрозы по маске not-a-virus:RemoteAdmin*** и **Добавить к исключениям файлы, рекомендованные Microsoft**.	Единый список исключений, который вы можете применять в выбранных задачах проверки по требованию и задаче **Постоянная защита файлов**. Глава 8 на стр. 108 содержит информацию о создании и применении доверенной зоны.

9.2.1. Область проверки в задачах проверки по требованию

В этом разделе содержится информация:

- о формировании области проверки (см. п. 9.2.1.1 на стр. 123);
- о предопределенных областях (см. п. 9.2.1.2 на стр. 124);
- как сформировать области проверки (см. п. 9.2.1.3 на стр. 126);
- как включить в область проверки сетевой путь (см. п. 9.2.1.4 на стр. 127);
- как создать виртуальную область проверки – включить в область проверки динамические диск, папку и файл (см. п. 9.2.1.5 на стр. 128).

9.2.1.1. О формировании области проверки в задачах проверки по требованию

По умолчанию в системной задаче **Полная проверка компьютера** и вновь созданных задачах проверки по требованию область проверки включен

весь сервер. Вы можете ограничить область проверки только некоторыми областями сервера, если по требованиям к безопасности нет необходимости проверять их все.

В консоли Антивируса область проверки представляет собой дерево файловых ресурсов сервера, которые Антивирус может проверять.

Узлы в дереве файловых ресурсов сервера отображаются следующим образом:

- ☑ Узел включен в область проверки.
- ☐ Узел исключен из области проверки.
- ☑ По крайней мере один из узлов, вложенных в этот узел, исключен из области проверки или параметры безопасности вложенного узла отличаются от параметров безопасности этого узла.

Имена виртуальных узлов области проверки отображаются шрифтом синего цвета.

9.2.1.2. Предопределенные области проверки

Чтобы просмотреть дерево файловых ресурсов сервера:

1. В дереве консоли разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, область проверки в которой вы хотите просмотреть, чтобы открыть задачу (см. рис. 41).

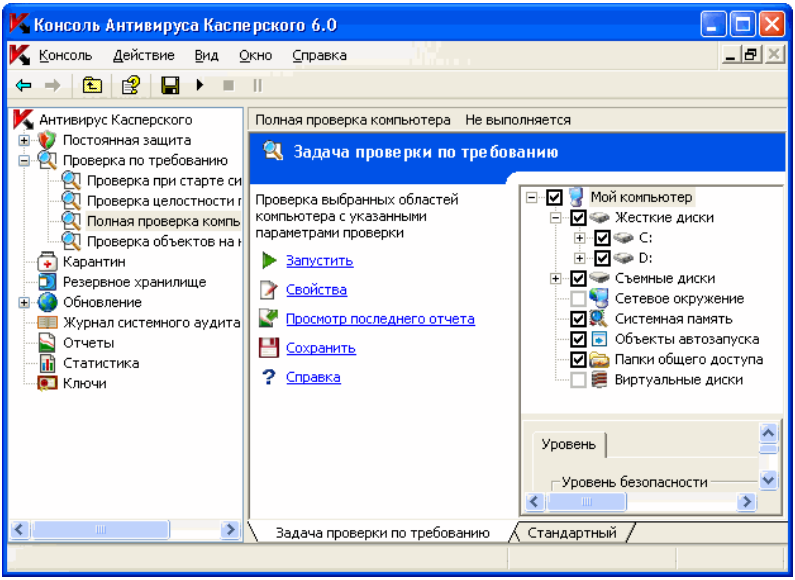

Рисунок 41. Пример дерева файловых ресурсов сервера в консоли Антивируса

В панели результатов отобразится дерево файловых ресурсов сервера, из объектов которого вы можете формировать область проверки.

Дерево файловых ресурсов сервера содержит следующие предопределенные области:

- **Мой компьютер**. Антивирус проверяет весь сервер.
- **Жесткие диски**. Антивирус проверяет объекты на жестких дисках сервера. Вы можете включать в область проверки или исключать из нее все жесткие диски, а также отдельные диски, папки или файлы.
- **Съемные диски**. Антивирус проверяет объекты на съемных носителях, например, компакт-дисках или USB-накопителях. Вы можете включать в область проверки или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Системная память**. Антивирус проверяет системную память и память процессов.
- **Объекты автозапуска**. Антивирус проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например,

WIN.INI или SYSTEM.INI, а также программные модули приложений, которые автоматически запускаются при старте компьютера.

- **Папки общего доступа**. Антивирус проверяет все папки общего доступа на защищаемом сервере.
- **Сетевое окружение**. Вы можете добавлять в область проверки сетевые папки или файлы, указывая пути к ним в формате UNC (Universal Naming Convention). Учетная запись, которую вы используете для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются под учетной записью **Локальная система** (**SYSTEM**). Подробнее см. в п. 9.2.1.4 на стр. 127.
- **Виртуальные диски**. Вы можете включать в область проверки динамические диски, папки и файлы, а также диски, которые монтируются на сервер, например: общие диски кластера (создавать *виртуальную область проверки*). Подробнее см. в п. 9.2.1.5 на стр. 128.

Примечание

Псевдодиски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов сервера в консоли Антивируса. Чтобы проверить объекты на псевдодиске, включите в область проверки папку на сервере, с которой этот псевдодиск связан.

Подключенные сетевые диски также не отображаются в дереве файловых ресурсов сервера. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

9.2.1.3. Формирование области проверки

Если вы управляете Антивирусом на защищаемом сервере удаленно, через консоль MMC, установленную на рабочем месте администратора, вы должны входить в группу локальных администраторов на защищаемом сервере, чтобы просматривать папки на нем.

Чтобы сформировать область проверки:

1. В дереве консоли разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, область проверки в которой вы хотите сформировать.

   В панели результатов отобразится дерево файловых ресурсов сервера. По умолчанию все области защищаемого сервера будут включены в область проверки.

3. Выполните следующие действия:

   - чтобы выбрать узлы, которые вы хотите включить в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:

     - если вы хотите включить в область проверки все диски одного типа, установите флажок рядом с названием нужного типа дисков;

     - если вы хотите включить в область проверки отдельный диск, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем нужного диска. Например, чтобы выбрать сменный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**;

     - если вы хотите включить в область проверки отдельную папку на диске, разверните дерево файловых ресурсов сервера, чтобы отобразить нужную папку, и установите флажок рядом с ее именем. Таким же образом вы можете включать в область проверки файлы;

   - чтобы исключить из области проверки отдельный узел, разверните дерево файловых ресурсов сервера, чтобы отобразить нужный узел, и снимите флажок рядом с его именем.

4. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

О том, как включить в область проверки:

- сетевой диск, папку или файл, см. п. 9.2.1.4 на стр. 127;
- динамический диск, папку или файл, см. п. 9.2.1.5 на стр. 128.

9.2.1.4. Включение в область проверки сетевых дисков, папок или файлов

Вы можете включать в область проверки сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Чтобы добавить в область проверки сетевой объект:

1. В дереве консоли разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, в область проверки которой вы хотите добавить сетевой путь.

3. Откройте контекстное меню на узле **Сетевое окружение** и выберите команду **Добавить сетевую папку** или команду **Добавить сетевой файл**.
4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention) и нажмите на клавишу **<ENTER>**.
5. Установите флажок рядом с добавленным сетевым объектом, чтобы включить его в область проверки.
6. Если требуется, измените параметры безопасности для добавленного сетевого объекта (см. п. 9.2.2 на стр. 130).
7. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

9.2.1.5. Создание виртуальной области проверки: включение в область проверки динамических дисков, папок или файлов

Вы можете включать в область проверки динамические диски, папки и файлы, а также диски, которые монтируются на сервер, например: общие диски кластера (создавать *виртуальную область проверки*). Подробнее о виртуальной области проверки читайте в п. 6.2.1.4 на стр. 74.

Вы можете добавлять в виртуальную область проверки динамические диски, папки или файлы.

Чтобы добавить в область проверки виртуальный диск:

1. В дереве консоли разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, в которой вы хотите создать виртуальную область проверки, чтобы открыть задачу.
3. В панели результатов, в дереве файловых ресурсов сервера, откройте контекстное меню на узле **Виртуальные диски** и в списке доступных имен выберите имя для создаваемого виртуального диска (см. рис. 42).

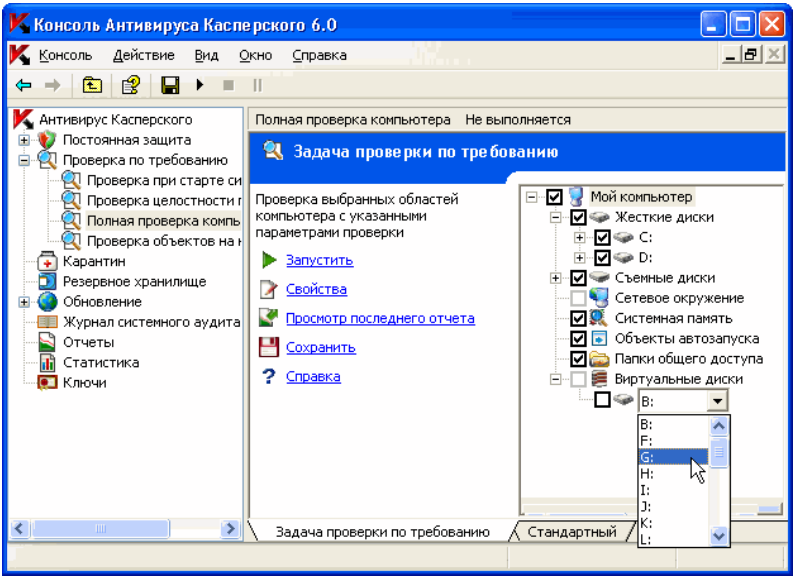

Рисунок 42. Выбор имени для создаваемого виртуального диска

4. Установите флажок рядом с добавленным диском, чтобы включить диск в область проверки.

5. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

Чтобы добавить в область проверки виртуальную папку или виртуальный файл:

1. В дереве консоли разверните узел **Проверка по требованию**.

2. Щелкните на задаче проверки по требованию, в которой вы хотите создать виртуальную область проверки, чтобы открыть задачу.

3. В панели результатов, в дереве файловых ресурсов сервера, откройте контекстное меню на узле, в который вы хотите добавить папку или файл, и выберите команду **Добавить виртуальную папку** или **Добавить виртуальный файл**.

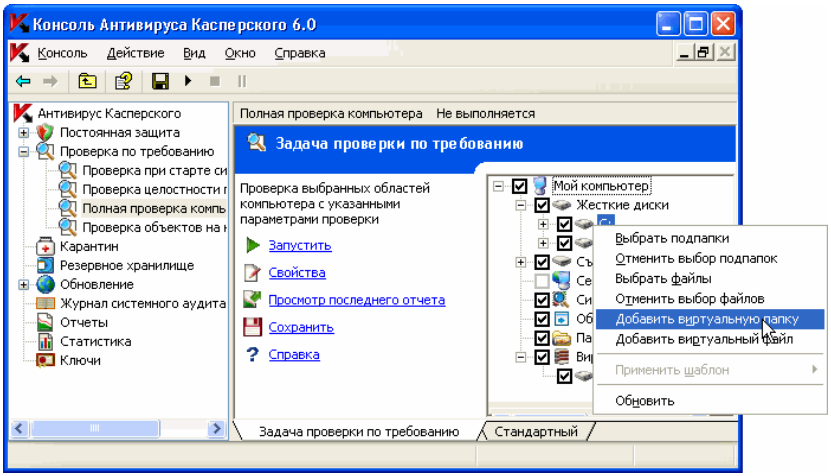

Рисунок 43. Добавление виртуальной папки

4. В поле ввода задайте имя для папки (файла). Вы можете задать маску имени папки (файла). Для маски используйте специальные символы * и ?.

5. В строке с названием созданной папки (созданного файла) установите флажок, чтобы включить папку (файл) в область проверки.

6. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

9.2.2. Настройка параметров безопасности для выбранного узла

В выбранной задаче проверки по требованию вы можете настроить параметры безопасности как едиными для всей области проверки, так и различными для разных узлов в дереве файловых ресурсов сервера. Параметры безопасности, которые вы настроите для выбранного узла, будут автоматически применяться для всех узлов, вложенных в него. Однако, если вы отдельно настроите параметры безопасности для вложенного узла, то параметры безопасности родительского узла для него применяться не будут.

Вы можете настроить параметры выбранной области проверки одним из следующих образов:

- выбрать один из трех предустановленных уровней безопасности (максимальная скорость, рекомендуемый или максимальная защита) (см. п. 9.2.2.1 на стр. 131);
- вручную изменить параметры безопасности выбранных узлов в дереве файловых ресурсов сервера (см. п. 9.2.2.2 на стр. 135).

Вы можете сохранить набор параметров узла в шаблон, чтобы потом применять этот шаблон для других узлов (см. п. 9.2.2.3 на стр. 139).

9.2.2.1. Выбор предустановленных уровней безопасности в задачах проверки по требованию

Для выбранного узла в дереве файловых ресурсов сервера вы можете задать один из трех предустановленных уровней безопасности: а) максимальная скорость, б) рекомендуемый и с) максимальная защита. Каждый из предустановленных уровней безопасности имеет свой набор значений параметров безопасности. Эти значения приведены в таблице 6.

Максимальная скорость

Вы можете установить уровень безопасности **Максимальная скорость**, если в вашей локальной сети, кроме использования Антивируса на серверах и рабочих станциях, принимаются дополнительные меры компьютерной безопасности, например, настроены сетевые экраны, действуют политики безопасности для пользователей сети.

Рекомендуемый

Уровень безопасности **Рекомендуемый** установлен по умолчанию. Он признан специалистами «Лаборатории Касперского» достаточным для проверки серверов в большинстве сетей. Этот уровень обеспечивает оптимальное сочетание качества проверки и ее скорости.

Максимальная защита

Используйте уровень безопасности **Максимальная защита**, если в вашей сети другие меры компьютерной безопасности не принимаются.

О том, как вручную настроить параметры безопасности для выбранного узла в дереве файловых ресурсов, см. п. 9.2.2 на стр. 130.

Таблица 6. Предустановленные уровни безопасности и соответствующие им значения параметров безопасности

Параметры	Предустановленный уровень безопасности		
	Максимальная скорость	**Рекомендуемый**	**Максимальная защита**
Проверяемые объекты (см. п. A.3.2 на стр. 400)	По формату	Все объекты	Все объекты
Проверка только новых и измененных объектов (см. п. A.3.3 на стр. 402)	Включена	Выключена	Выключена
Действие над зараженными объектами (см. п. A.3.5 на стр. 404)	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно
Действие над подозрительными объектами (см. п. A.3.6 на стр. 407)	Помещать на карантин	Помещать на карантин	Помещать на карантин
Исключение объектов (см. п. A.3.8 на стр. 411)	Нет	Нет	Нет
Исключение угроз (см. п. A.3.9 на стр. 412)	Нет	Нет	Нет
Макс. продолжительность проверки объекта (см. п. A.3.10 на стр. 414)	60 сек.	Нет	Нет

Параметры	Предустановленный уровень безопасности		
	Максимальная скорость	**Рекомендуемый**	**Максимальная защита**
Макс. размер проверяемого составного объекта (см. п. A.3.11 на стр. 415)	8 МБ	Нет	Нет
Проверка дополнительных потоков файловой системы (NTFS) (см. п. A.3.2 на стр. 400)	Да	Да	Да
Проверка загрузочных секторов (см. п. A.3.2 на стр. 400)	Да	Да	Да
Проверка составных объектов (см. п. A.3.4 на стр. 403)	• SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* * Только новые и измененные	• Архивы* • SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* * Все объекты	• Архивы* • SFX-архивы* • почтовые базы* • файлы почтовых форматов* • упакованные объекты* • вложенные OLE-объекты* * Все объекты

Примечание

Обратите внимание, что параметры безопасности **Применение технологии iChecker** и **Применение технологии iSwift** не входят в набор параметров предустановленных уровней безопасности. По умолчанию эти параметры включены. Если вы измените состояние параметров **Применение технологии iChecker** и **Применение технологии iSwift**, выбранный вами предустановленный уровень безопасности не изменится.

Чтобы выбрать один из предустановленных уровней безопасности:

1. В дереве консоли выберите узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, в которой вы хотите настроить параметры безопасности.
3. В панели результатов выберите узел области проверки, для которого вы хотите выбрать предустановленный уровень безопасности.
4. Убедитесь, что этот узел включен в область проверки (см. п. 9.2.1.1 на стр. 123).
5. В диалоговом окне **Уровень безопасности** (см. рис. 44) выберите уровень, который вы хотите применить.

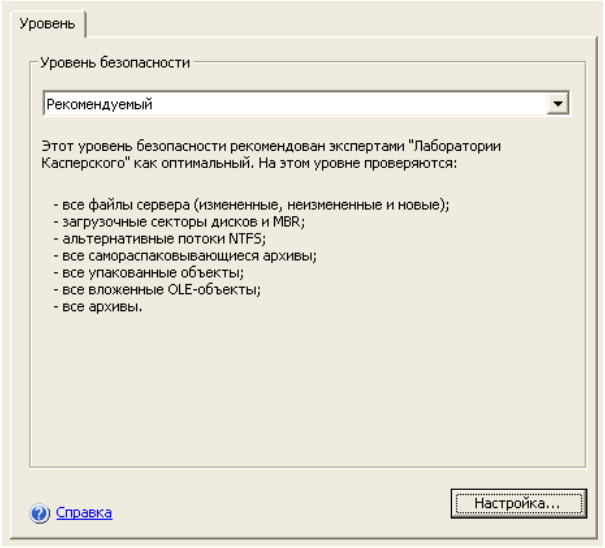

Рисунок 44. Диалоговое окно **Уровень безопасности**

В диалоговом окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.

6. Откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

9.2.2.2. Настройка параметров безопасности вручную

Чтобы вручную настроить параметры безопасности:

1. В дереве консоли выберите узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, в которой вы хотите настроить параметры безопасности.
3. В панели результатов выберите узел области проверки, параметры безопасности которого вы хотите настроить. Убедитесь, что этот узел включен в область проверки (подробнее о формировании области проверки читайте в п. 9.2.1.3 на стр. 126).

   В нижней части панели результатов отобразится диалоговое окно **Уровень безопасности** (см. рис. 45).

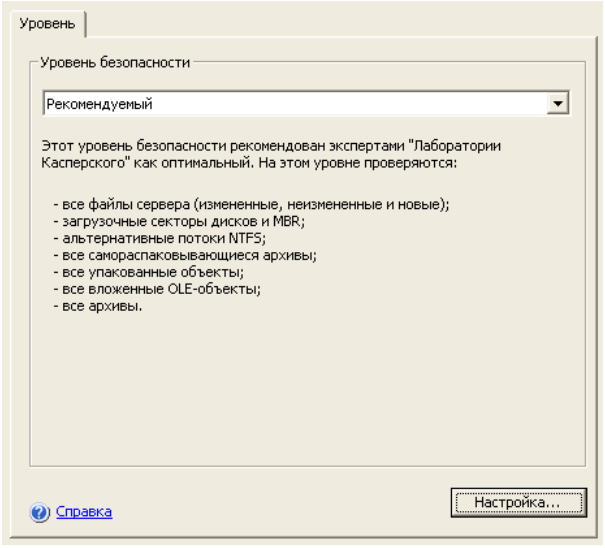

Рисунок 45. Диалоговое окно **Уровень безопасности**

Нажмите на кнопку **Настройка**, чтобы открыть диалоговое окно **Параметры безопасности**.

Примечание

Вы можете открыть диалоговое окно **Параметры безопасности** для выбранного узла в дереве файловых ресурсов, открыв контекстное меню на этом узле и выбрав **Свойства**.

4. В диалоговом окне **Параметры безопасности** настройте нужные параметры безопасности выбранного узла в соответствии с вашими требованиями.

   - На закладке **Общие** (см. рис. 46) выполните следующие действия:

     - под заголовком **Проверка объектов** укажите, будет ли Антивирус проверять все объекты области проверки или только объекты с определенными форматами или расширениями, будет ли он проверять загрузочные секторы дисков и главную загрузочную запись, альтернативные потоки NTFS (см. п. A.3.2 на стр. 400);

     - под заголовком **Оптимизация** укажите, будет ли Антивирус проверять все объекты в выбранной области или только новые и измененные (см. п. A.3.3 на стр. 402);

     - под заголовком **Проверка составных объектов** укажите, какие составные объекты Антивирус будет проверять (см. п. A.3.4 на стр. 403).

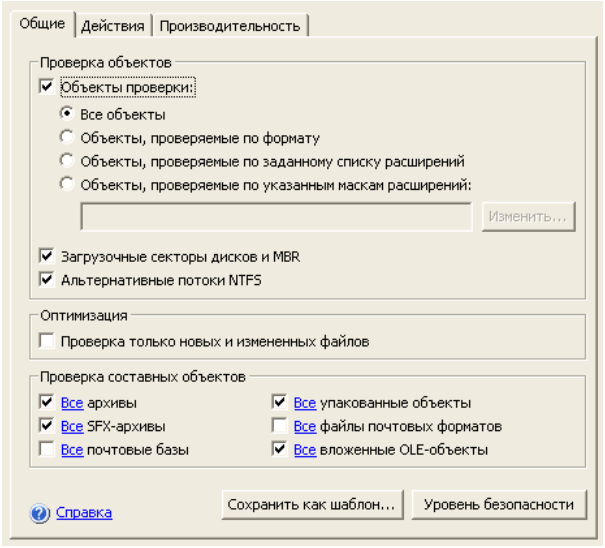

Рисунок 46. Диалоговое окно **Параметры безопасности** задачи **Проверка по требованию**, закладка **Общие**

- На закладке **Действия** (см. рис. 47) выполните следующие действия:
  - выберите действие над зараженными объектами (см. п. А.3.5 на стр. 404);
  - выберите действие над подозрительными объектами (см. п. А.3.6 на стр. 407);
  - если требуется, настройте действия над объектами в зависимости от типа обнаруженной в объекте угрозы (см. п. А.3.7 на стр. 409).

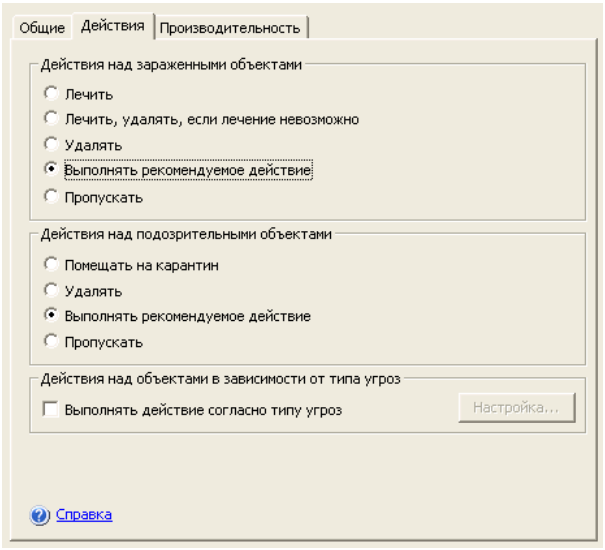

Рисунок 47. Диалоговое окно **Параметры безопасности** задачи **Проверка по требованию**, закладка **Действия**

- На закладке **Производительность** (см. рис. 48), если требуется, выполните следующие действия:
  - исключите из обработки файлы по имени или маске (см. п. A.3.8 на стр. 411);
  - исключите из обработки угрозы по названиям или маскам названий (см. п. A.3.9 на стр. 412);
  - укажите максимальную продолжительность проверки объекта (см. п. A.3.10 на стр. 414);
  - укажите максимальный размер проверяемого составного объекта (см. п. A.3.11 на стр. 415);
  - включите или выключите применение технологии iChecker (см. п. A.3.12 на стр. 416);
  - включите или выключите применение технологии iSwift (см. п. A.3.13 на стр. 417).

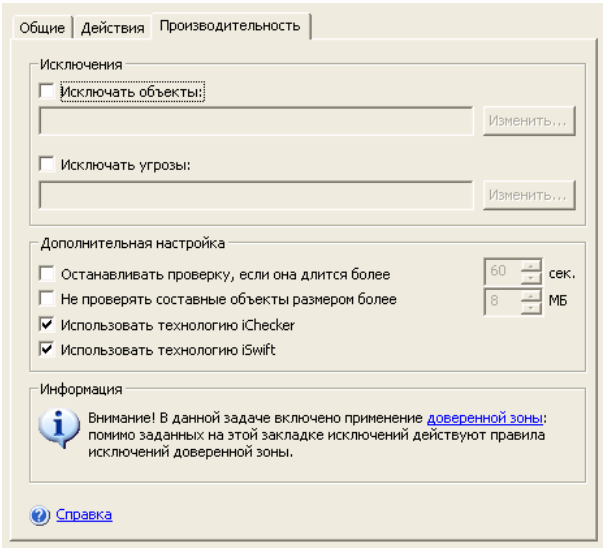

Рисунок 48. Диалоговое окно **Параметры безопасности** задачи **Проверка по требованию**, закладка **Производительность**

5. После того как вы настроите нужные параметры безопасности, откройте контекстное меню на имени задачи и выберите команду **Сохранить задачу**, чтобы сохранить изменения в задаче.

9.2.2.3. Работа с шаблонами в задачах проверки по требованию

В этом разделе содержится следующая информация:

- сохранение набора параметров безопасности в шаблон (см. п. 9.2.2.3.1 на стр. 140);
- просмотр параметров безопасности в шаблоне (см. п. 9.2.2.3.2 на стр. 141);
- применение шаблона (см. п. 9.2.2.3.3 на стр. 142);
- удаление шаблона (см. п. 9.2.2.3.4 на стр. 143).

9.2.2.3.1. Сохранение набора параметров безопасности в шаблон

В задаче проверки по требованию, после того как вы настроили параметры безопасности какого-либо узла в дереве файловых ресурсов сервера, вы можете сохранить этот набор параметров в шаблон, чтобы потом применять его для других узлов в этой или других задачах проверки по требованию.

Чтобы сохранить набор параметров безопасности в шаблон:

1. В дереве консоли выберите узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, параметры безопасности в которой вы хотите сохранить в шаблон.
3. В дереве файловых ресурсов сервера выберите узел, набор параметров безопасности которого вы хотите сохранить.
4. В диалоговом окне **Параметры безопасности** на закладке **Общие** нажмите на кнопку **Сохранить как шаблон**.
5. В диалоговом окне **Свойства шаблона** (см. рис. 49) выполните следующие действия:
   - В поле **Имя шаблона** введите название шаблона.
   - В поле **Описание** введите любую дополнительную информацию о шаблоне.

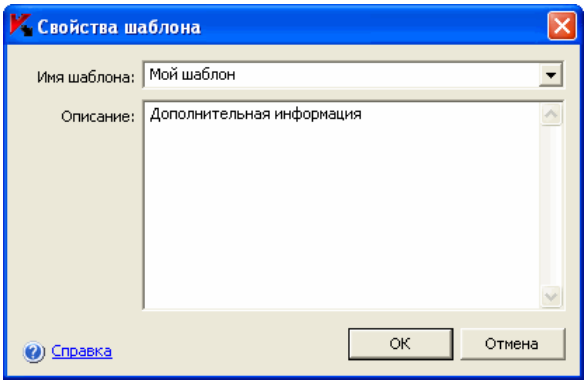

Рисунок 49. Диалоговое окно **Свойства шаблона**

6. Нажмите на кнопку **ОК**. Шаблон с набором значений параметров будет сохранен.

9.2.2.3.2. Просмотр параметров безопасности в шаблоне

Чтобы просмотреть значения параметров безопасности в созданном шаблоне:

1. В дереве консоли откройте контекстное меню на узле **Проверка по требованию** и выберите команду **Шаблоны** (см. рис. 50).

Рисунок 50. Диалоговое окно **Шаблоны**

В диалоговом окне **Шаблоны** отображается список шаблонов, которые вы можете применить в задачах проверки по требованию.

2. Чтобы просмотреть информацию о шаблоне и значения параметров безопасности в нем, выберите нужный шаблон в списке и нажмите на кнопку **Просмотреть** (см. рис. 51).

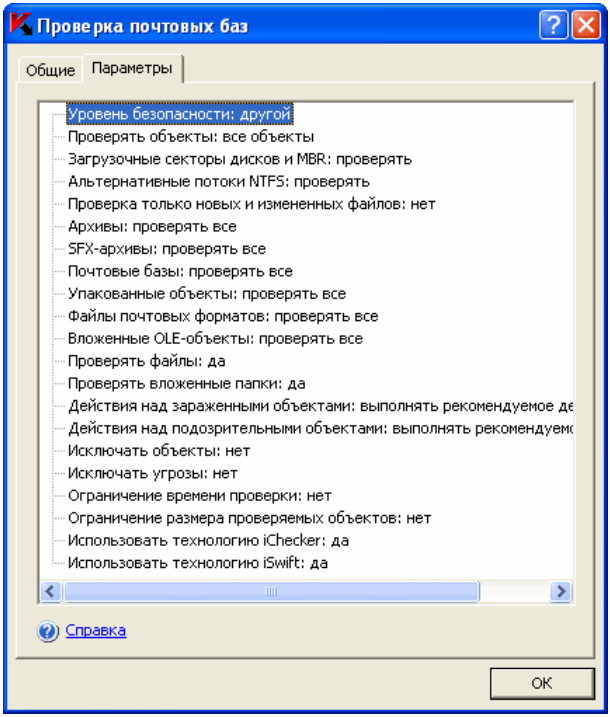

Рисунок 51. Диалоговое окно **<Имя шаблона>**, закладка **Параметры**

На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне; на закладке **Параметры** приводится список значений параметров безопасности, сохраненных в шаблоне.

9.2.2.3.3. Применение шаблона

Чтобы применить шаблон с параметрами безопасности:

1. Предварительно сохраните набор параметров безопасности в шаблон (см. инструкцию в п. 9.2.2.3.1 на стр. 140).
2. В дереве консоли выберите узел **Проверка по требованию**.
3. Выберите задачу проверки по требованию, в которой вы хотите применить параметры безопасности из шаблона.
4. В дереве файловых ресурсов сервера откройте контекстное меню на узле, для которого вы хотите применить шаблон, и выберите **Применить шаблон** → **Список шаблонов**.

5. В списке шаблонов выберите шаблон, который вы хотите применить.

6. В диалоговом окне **Параметры безопасности** нажмите на кнопку **ОК**, чтобы сохранить изменения.

Примечание

Если вы примените шаблон к родительскому узлу, то параметры безопасности из шаблона применятся также ко всем вложенным узлам, кроме тех узлов, для которых вы настраивали параметры безопасности отдельно.

Чтобы установить параметры безопасности из шаблона ко всем вложенным узлам, перед применением шаблона снимите флажок с родительского узла в дереве файловых ресурсов сервера, а затем снова установите его. Примените шаблон к родительскому узлу. Все вложенные узлы будут иметь такие же параметры безопасности, как и родительский узел.

9.2.2.3.4. Удаление шаблона

Чтобы удалить шаблон:

1. В дереве консоли откройте контекстное меню на узле **Проверка по требованию** и выберите команду **Шаблоны** (см. рис. 50).

2. В диалоговом окне **Шаблоны** в списке шаблонов выберите шаблон, который вы хотите удалить, и нажмите на кнопку **Удалить**.

3. В диалоговом окне подтверждения нажмите на кнопку **Да**. Выбранный шаблон будет удален.

9.3. Выполнение задачи проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Антивируса, имеют базовый приоритет **Средний** (**Normal**).

Вы можете присвоить процессу, в котором будет выполняться задача проверки по требованию, базовый приоритет **Низкий** (**Low**). Понижение приоритета процесса увеличивает время выполнения задачи, но оно также может положительно повлиять на скорость выполнения процессов других активных приложений.

В одном рабочем процессе с низком приоритетом может выполняться несколько задач в фоновом режиме. Вы можете установить максимальное количество процессов для фоновых задач проверки по требованию (см. п. A.1.3 на стр. 376).

Вы можете указать приоритет задачи при ее создании или позже, в диалоговом окне **Свойства задачи**.

Чтобы изменить приоритет задачи проверки по требованию:

1. В дереве консоли разверните узел **Проверка по требованию**.
2. Откройте контекстное меню на задаче проверки по требованию, приоритет которой вы хотите изменить, и выберите команду **Свойства**.

   Откроется диалоговое окно **Свойства задачи** (см. рис. 52).

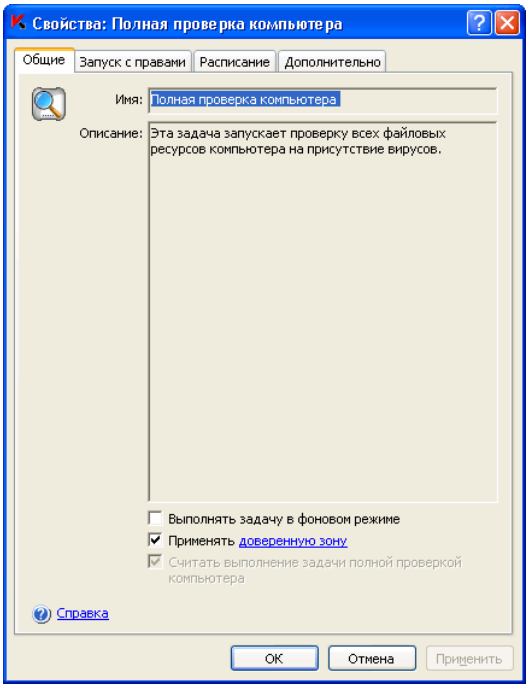

Рисунок 52. Диалоговое окно **Свойства задачи**

3. На закладке **Общие** выполните одно из следующих действий:
   - чтобы включить фоновый режим выполнения задачи, установите флажок **Выполнять задачу в фоновом режиме**;

- чтобы отключить фоновый режим выполнения задачи, снимите флажок **Выполнять задачу в фоновом режиме**.

Примечание

Если вы включите или выключите фоновый режим выполняющейся задачи, то приоритет задачи изменится не сразу, а только при ее последующем запуске.

9.4. Статистика задач проверки по требованию

Пока выполняется задача проверки по требованию, вы можете просматривать в диалоговом окне **Статистика** информацию о количестве объектов, которые Антивирус обработал с момента запуска задачи по текущий момент.

Информация в диалоговом окне **Статистика** будет доступна, если вы приостановите задачу. После завершения или остановки задачи вы сможете просмотреть эту информацию в подробном отчете о событиях в задаче (см. п. 13.2.4 на стр. 209).

Чтобы просмотреть статистику задачи проверки по требованию:

1. В дереве консоли разверните узел **Проверка по требованию**.
2. Откройте контекстное меню на задаче проверки по требованию, статистику которой вы хотите просмотреть, и выберите команду **Просмотреть статистику** (см. рис. 53).

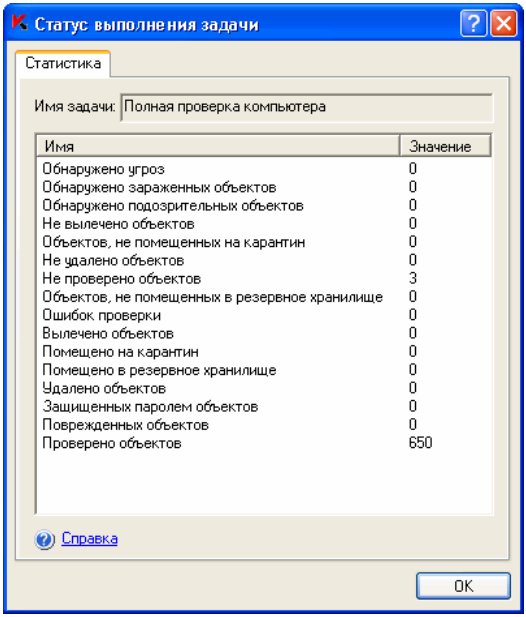

Рисунок 53. Диалоговое окно **Статус выполнения задачи**

В диалоговом окне **Статус выполнения задачи** отображается следующая информация об объектах, которые Антивирус обработал с момента запуска задачи по текущий момент:

- в задаче **Проверка целостности приложения**:

Поле	Описание
Модулей с нарушением целостности	Количество модулей, целостность которых нарушена Если обнаружены модули с нарушением целостности, выполните восстановление Антивируса. См. инструкцию в документе *Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство по установке.*
Всего проверено модулей	Общее количество проверенных модулей

- в задачах **Полная проверка компьютера**, **Проверка при старте системы**, **Проверка объектов на карантине** и пользовательских задачах проверки по требованию:

Поле	Описание
Обнаружено угроз	Количество обнаруженных угроз; например, если Антивирус обнаружит в пяти объектах одну вредоносную программу, значение в этом поле увеличится на единицу.
Обнаружено зараженных объектов	Общее количество обнаруженных зараженных объектов.
Обнаружено подозрительных объектов	Общее количество обнаруженных подозрительных объектов.
Не вылечено объектов	Количество объектов, которые Антивирус не вылечил, так как: а) тип угрозы в объекте не предполагает его лечения; б) объекты этого типа не могут быть вылечены; в) при лечении возникла ошибка.
Объектов, не помещенных на карантин	Количество объектов, которые Антивирус должен был поместить на карантин, но ему это не удалось из-за ошибки, например, из-за отсутствия свободного места на диске.
Не удалено объектов	Количество объектов, которые Антивирус пытался удалить, но ему это не удалось, так как, например, доступ к объекту был заблокирован другой программой.
Не проверено объектов	Количество объектов в области проверки, которые Антивирусу проверить не удалось, так как, например, доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество файлов, копии которых Антивирус должен был сохранить в резервном хранилище, но это ему не удалось из-за ошибки.
Ошибок проверки	Количество объектов, во время обработки которых возникла ошибка Антивируса.

Поле	Описание
Вылечено объектов	Количество объектов, которые Антивирус вылечил.
Помещено на карантин	Количество объектов, которые Антивирус поместил на карантин.
Помещено в резервное хранилище	Количество файлов, копии которых Антивирус сохранил в резервном хранилище.
Удалено объектов	Количество объектов, которые Антивирус удалил.
Защищенных паролем объектов	Количество объектов (например, архивов), которые Антивирус пропустил, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, пропущенных Антивирусом, так как их формат искажен.
Проверено объектов	Общее количество объектов, проверенных Антивирусом.

ГЛАВА 10. ОБНОВЛЕНИЕ БАЗ И ПРОГРАММНЫХ МОДУЛЕЙ АНТИВИРУСА

В этом разделе содержится следующая информация:

10.1. Об обновлении баз Антивируса

Базы Антивируса, хранящиеся на защищаемом сервере, быстро становятся неактуальными. Вирусные аналитики «Лаборатории Касперского» ежедневно обнаруживают сотни новых угроз, создают идентифицирующие их записи и включают их в обновления баз. (*Обновление баз* представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента создания предыдущего

обновления). Чтобы свести риск заражения сервера к минимуму, регулярно получайте обновления баз.

По умолчанию, если базы Антивируса не обновляются в течение недели с момента создания последних установленных обновлений баз, возникает событие *Базы устарели*, а если базы не обновляются в течение двух недель, возникает событие *Базы сильно устарели* (информация об актуальности баз отображается в узле **Статистика**, см. п. 13.4 на стр. 221). Вы можете указать другое количество дней перед наступлением этих событий с помощью общих параметров Антивируса (см. п. 3.2 на стр. 46), а также настроить уведомления администратора об этих событиях (см. п. 15.2 на стр. 237).

Вы можете обновлять базы с FTP или HTTP-*серверов обновлений* «Лаборатории Касперского» или других источников обновлений, используя задачу Антивируса **Обновление баз приложения**. Подробнее о задаче **Обновление баз приложения**, читайте в п. 10.4 на стр. 157.

Вы можете загружать обновления на каждый защищаемый сервер или использовать один компьютер в качестве посредника, копируя обновления на него и затем распределяя их на серверы. А если вы используете приложение Kaspersky Administration Kit для централизованного управления защитой компьютеров в организации, вы можете использовать Сервер администрирования Kaspersky Administration Kit в качестве посредника для загрузки обновлений. Чтобы копировать базы на компьютер-посредник без их применения, используйте задачу **Копирование обновлений**. Подробнее об этой задаче читайте в п. 10.4 на стр. 157.

Вы можете запускать задачи обновления баз вручную или по расписанию (о том, как настроить расписание задачи, см. п. 5.7 на стр. 60).

Если загрузка обновлений прервется или завершится с ошибкой, Антивирус автоматически вернется к использованию баз с последними установленными обновлениями. А в случае повреждения баз Антивируса, вы можете сами *откатить их* до предыдущих установленных обновлений (см. п. 10.7 на стр. 168).

Примечание

Если у вас нет доступа к интернету, вы можете получать файлы обновлений на дискетах или компакт-дисках у наших партнеров. Информация о партнере, у которого вы приобрели Антивирус, отображается в консоли Антивируса, в свойствах установленного ключа. Вы также можете узнать адрес ближайшего к вам партнера в нашем центральном офисе в Москве по телефонам +7 (495) 797-87-07, +7 (495) 645-79-29 или +7 (495) 956-87-08 (обслуживание ведется на русском и английском языках).

10.2. Об обновлении программных модулей Антивируса

«Лаборатория Касперского» может выпускать пакеты обновлений программных модулей Антивируса. Пакеты обновлений делятся на срочные (или критические) и плановые. *Срочные* пакеты обновлений устраняют уязвимости; *плановые* добавляют новые функции или улучшают существующие.

Срочные пакеты обновлений публикуются на серверах обновлений «Лаборатории Касперского». Вы можете автоматически загружать и устанавливать их, настроив системную задачу **Обновление модулей приложения**.

«Лаборатория Касперского» не публикует плановые пакеты обновлений на серверах обновлений для автоматизированной установки; вы можете загружать их с веб-сайта «Лаборатории Касперского». Вы можете получать информацию о выходе плановых обновлений Антивируса с помощью задачи **Обновление модулей приложения**.

Вы можете загружать срочные обновления из интернета на каждый защищаемый сервер или использовать один компьютер в качестве посредника, копируя обновления на него без их установки, а затем распределяя их на серверы. Чтобы копировать и сохранять обновления без их установки, используйте задачу **Копирование обновлений**. Подробнее об этой задаче читайте в п. 10.4 на стр. 157.

Перед тем как установить обновления программных модулей, Антивирус создает резервные копии модулей, установленных ранее. Если обновление программных модулей прервется или завершится с ошибкой, Антивирус автоматически вернется к использованию ранее установленных программных модулей. Вы также можете *откатить программные модули вручную до предыдущих установленных обновлений* (см. п. 10.8 на стр. 168).

На время установки полученных обновлений служба Антивируса автоматически останавливается, а затем снова запускается.

Примечание

Если у вас нет доступа к интернету, вы можете получать файлы обновлений на дискетах или компакт-дисках у наших партнеров. Информация о партнере, у которого вы приобрели Антивирус, отображается в консоли Антивируса, в свойствах установленного ключа. Вы также можете узнать адрес ближайшего к вам партнера в нашем центральном офисе в Москве по телефонам +7 (495) 797-87-07, +7 (495) 645-79-29 или +7 (495) 956-87-08 (обслуживание ведется на русском и английском языках).

10.3. Схемы обновления баз и программных модулей антивирусных приложений в организации

Ваш выбор источника обновлений в задачах обновления зависит от того, какую схему обновления баз и модулей антивирусных приложений вы используете в организации.

Вы можете обновлять базы и модули Антивируса на защищаемых серверах по следующим схемам:

- загружать обновления напрямую из интернета на каждый защищаемый сервер (**схема 1**);
- загружать обновления из интернета на компьютер-посредник и с него распределять на серверы.

  Посредником может служить любой компьютер, на котором установлен:

  - Антивирус (один из защищаемых серверов) (**схема 2**)

    или

  - Сервер администрирования Kaspersky Administration Kit (**схема 3**).

  Обновление через компьютер-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность серверов.

Перечисленные схемы обновлений описаны ниже.

Схема 1. Обновление напрямую из интернета

На каждом защищаемом сервере настройте задачу **Обновление баз приложения** (**Обновление модулей приложения**). В качестве источника обновлений укажите серверы обновлений «Лаборатории Касперского». Настройте расписание задачи.

Вы можете указать в качестве источника другие HTTP- или FTP- серверы, которые содержат папку с файлами обновлений.

Рисунок 54. Обновление напрямую из интернета

Схема 2. Обновление через один из защищаемых серверов

Обновление по этой схеме (см. рис. 55) включает следующие шаги:

Шаг 1. Копирование обновлений на выбранный защищаемый сервер

На выбранном сервере настройте задачу **Копирование обновлений**. В качестве источника обновлений укажите серверы обновлений «Лаборатории Касперского». Укажите папку, в которой будут сохранены обновления: это должна быть папка общего доступа.

Используя эту задачу, вы можете также получать обновления не только для защищаемых серверов, но и компьютеров локальной сети, на которых установлены другие приложения «Лаборатории Касперского» версии 6.0 (например, Антивирус Касперского 6.0 для Windows Workstations).

Шаг 2. Распределение обновлений на остальные защищаемые серверы

Настройте на каждом из защищаемых серверов задачу **Обновление баз приложения** (**Обновление модулей приложения**). В ней в качестве источника обновлений укажите папку на диске компьютера-посредника, в которую вы скопировали обновления.

Рисунок 55. Обновление через один из защищаемых серверов

Схема 3. Обновление через Сервер администрирования Kaspersky Administration Kit

Если вы используете приложение Kaspersky Administration Kit для централизованного управления защитой компьютеров, вы можете загружать обновления через Сервер администрирования Kaspersky Administration Kit (см. рис. 56).

Рисунок 56. Обновление через Сервер администрирования Kaspersky Administration Kit.

Обновление по этой схеме включает следующие шаги:

Шаг 1. Загрузка обновлений с сервера обновлений «Лаборатории Касперского» на Сервер администрирования Kaspersky Administration Kit

Настройте глобальную задачу **Получение обновлений Сервером администрирования**. В качестве источника обновлений укажите серверы обновлений «Лаборатории Касперского».

Вы можете получать обновления не только для защищаемых серверов, но и других компьютеров локальной сети, на которых установлены другие приложения «Лаборатории Касперского» версии 6.0 (например, Антивирус Касперского 6.0 для Windows Workstations).

Шаг 2. Распределение обновлений на защищаемые серверы

Распределите обновления на защищаемые серверы одним из следующих способов:

- Настройте на Сервере администрирования Kaspersky Administration Kit групповую задачу обновления баз Антивируса (программных модулей) для распределения обновлений на защищаемые серверы; в расписании задачи укажите частоту запуска **При получении обновлений Сервером администрирования**. Сервер администрирования

рирования будет запускать задачу каждый раз, как только он получит обновления (этот способ является рекомендуемым).

Настройте расписание задачи. Для задачи, созданной в Консоли администрирования вы можете указать частоту запуска **После получения обновлений Сервером администрирования**. Задача будет запускаться каждый раз, как только Сервер администрирования получит обновления баз.

> **Примечание**
>
> Вы не можете указывать частоту запуска **После получения обновлений Сервером администрирования** в консоли Антивируса в MMC.

- Настройте на каждом из защищаемых серверов задачу **Обновление баз приложения** (**Обновление модулей приложения**); в ней в качестве источника обновлений выберите Сервер администрирования Kaspersky Administration Kit. Настройте расписание задачи.

Если вы планируете использовать Сервер администрирования Kaspersky Administration Kit для распределения обновлений, предварительно установите на каждом из защищаемых серверов программный компонент Агент администрирования, который входит в комплект поставки приложения Kaspersky Administration Kit. Он обеспечивает взаимодействие между Сервером администрирования и Антивирусом на защищаемом сервере. Подробнее об Агенте администрирования и его настройке с помощью приложения Kaspersky Administration Kit читайте в документе *Kaspersky Administration Kit. Руководство администратора*.

10.4. Задачи обновления

В Антивирусе предусмотрены четыре системные задачи обновления: **Обновление баз приложения**, **Обновление модулей приложения**, **Копирование обновлений** и **Откат обновления баз** (см. рис. 57).

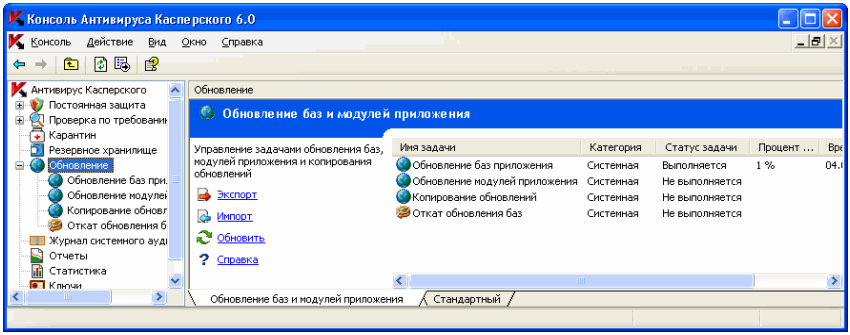

Рисунок 57. Задачи обновления в окне консоли Антивируса

Обновление баз приложения

Антивирус копирует базы из источника обновлений на защищаемый сервер и сразу переходит к их использованию в выполняющихся задачах постоянной защиты и проверки по требованию.

По умолчанию Антивирус запускает задачу **Обновление баз приложения** каждый час; он соединяется с источником обновлений – одним из серверов обновлений «Лаборатории Касперского», – автоматически определяя параметры прокси-сервера в сети и не используя проверку подлинности при доступе к прокси-серверу.

Обновление модулей приложения

Антивирус копирует обновления своих программных модулей из источника обновлений на защищаемый сервер и устанавливает их. Для применения установленных программных модулей может потребоваться перезагрузка компьютера и/или перезапуск Антивируса.

Еженедельно, по пятницам в 16:00 (время в формате, установленном региональными настройками защищаемого сервера) Антивирус запускает задачу **Обновление модулей приложения**, чтобы только проверить наличие критических и плановых обновлений модулей Антивируса, не копируя их.

Копирование обновлений

Антивирус загружает файлы обновлений баз и программных модулей и сохраняет их в указанную сетевую или локальную папку, не применяя.

Откат обновления баз

Антивирус возвращается к использованию баз с предыдущими установленными обновлениями.

О том, как настроить задачи обновления, см. п. 10.5 на стр. 158.

Примечание

Вы можете останавливать задачи обновления, однако вы не можете приостанавливать их.

О том, как управлять задачами в Антивирусе см. в п. 5.6 на стр. 59.

10.5. Настройка задач обновления

В этом разделе описано, как выполнить следующие действия в задачах обновления:

- выбрать источник обновлений, настроить соединение с источником обновлений, указать местоположение защищаемого сервера для оптимизации получения обновлений (эти параметры имеются в каждой задаче обновления) (см. п. 10.5.1 на стр. 158);
- настроить параметры задачи *Обновление модулей приложения* (см. п. 10.5.2 на стр. 163);
- настроить параметры задачи *Копирование обновлений* (см. п. 10.5.3 на стр. 165).

10.5.1. Выбор источника обновлений, настройка соединения с источником обновлений и региональные настройки

В каждой из задач обновления вы можете указать один или несколько источников обновлений, настроить параметры соединения с источниками, а также указать местоположение защищаемого сервера для оптимизации получения обновлений (региональные настройки).

Чтобы настроить параметры обновления:

1. В дереве консоли выберите **Обновление**.
2. Откройте контекстное меню на задаче обновления, в которой вы хотите настроить источник обновлений, и выберите команду **Свойства**.

   На закладках диалогового окна **Свойства задачи** настройте параметры обновления в соответствии с вашими требованиями.
3. На закладке **Общие** (см. рис. 58) выберите источник, из которого вы хотите получать обновления (подробнее о параметре читайте в п. A.5.1 на стр. 426).

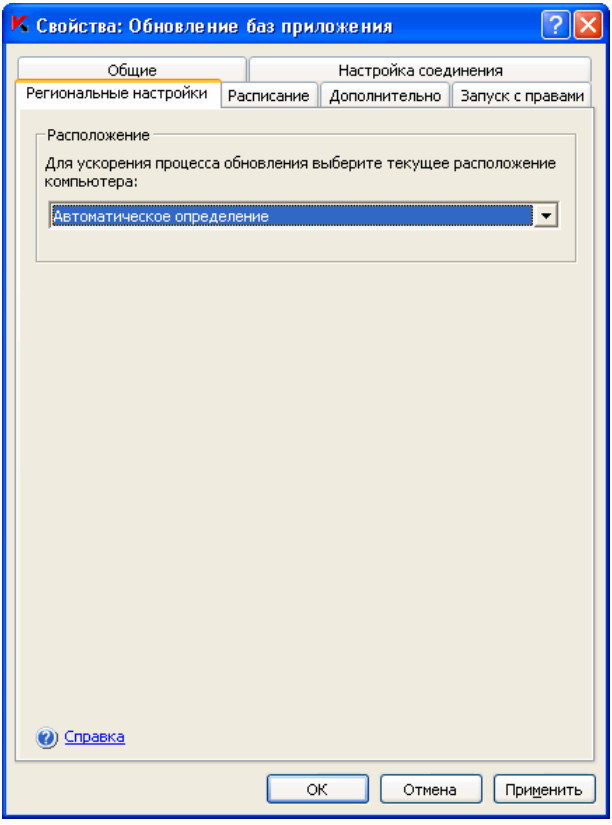

Рисунок 58. Диалоговое окно **Свойства задачи**, закладка **Общие**

4. Если вы выбрали **Другие HTTP-, FTP-серверы или сетевые ресурсы**, добавьте один или несколько пользовательских источников обновлений. Чтобы указать источник, нажмите на кнопку **Изменить** и в диалоговом окне **Серверы обновлений** (см. рис. 59) нажмите на кнопку **Добавить** и в поле ввода укажите адрес папки с файлами обновлений на FTP- или HTTP- сервере; укажите локальную или сетевую папку в формате UNC (Universal Naming Convention). Нажмите на кнопку **ОК**.

   Вы можете включать или отключать добавленные пользовательские источники: чтобы отключить добавленный источник, снимите флажок рядом с ним в списке; чтобы включить источник, установите флажок рядом с ним в списке.

   Чтобы изменить очередность обращения Антивируса к пользовательским источникам, с помощью кнопок **Вверх** и **Вниз** перемещайте выбранный источник к началу или концу списка в зависимости от того, хотите вы использовать его раньше или позже.

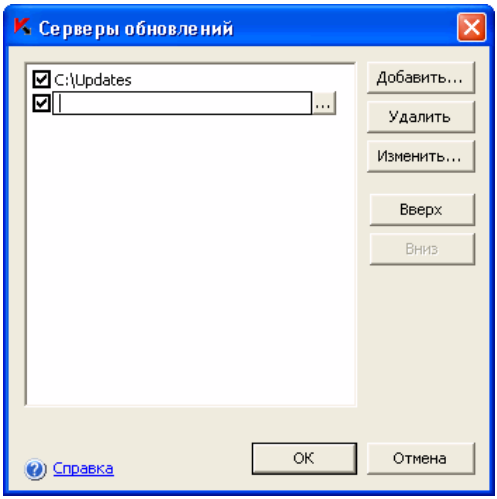

Рисунок 59. Добавление пользовательских источников обновления

   Чтобы изменить путь к источнику, выберите источник в списке и нажмите на кнопку **Изменить**, выполните нужные изменения в поле ввода и нажмите на клавишу **<ENTER>**.

   Чтобы удалить источник, выберите его в списке и нажмите на кнопку **Удалить**. Источник будет удален из списка.

5. Чтобы использовать для получения обновлений серверы обновлений «Лаборатории Касперского» в случае, если пользовательские

источники окажутся недоступными, установите флажок **Использовать серверы обновлений «Лаборатории Касперского», если источники, указанные пользователем, недоступны**.

6. На закладке **Настройка соединения** (см. рис. 60) настройте соединение с источником обновлений.

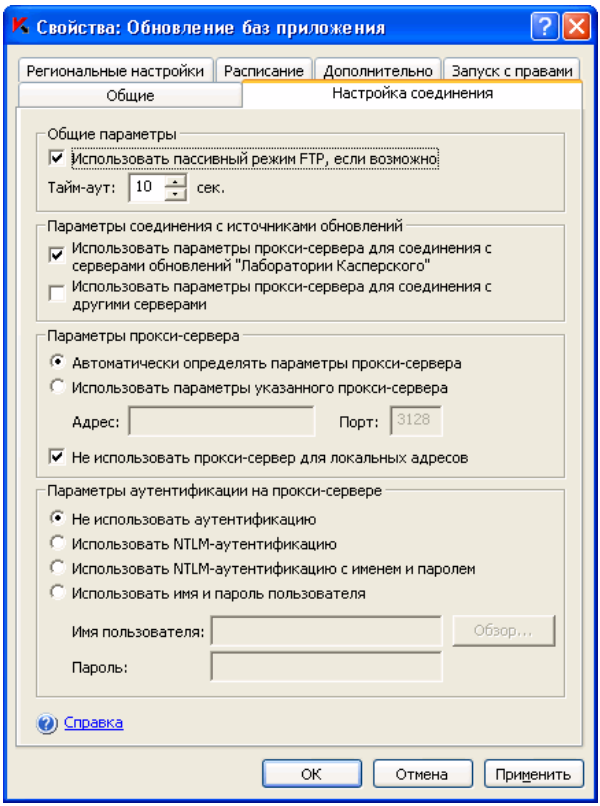

Рисунок 60. Диалоговое окно **Свойства задачи**, закладка **Настройка соединения**

Выполните следующие действия:

- укажите режим FTP-сервера для соединения с защищаемым сервером (см. п. A.5.2 на стр. 427);
- если требуется, измените время ожидания при соединении с источником обновлений (см. п. A.5.3 на стр. 428);

- если для получения обновлений с какого-либо из указанных источников требуется доступ к прокси-серверу, то опишите параметры доступа к прокси-серверу:
  - обращение к прокси-серверу при подключении к различным источникам обновлений (см. п. A.5.4.1 на стр. 429);
  - адрес прокси-сервера (см. п. A.5.4.2 на стр. 430);
  - метод проверки подлинности при доступе к прокси-серверу (см. п. A.5.4.3 на стр. 431).

7. На закладке **Региональные настройки** (см. рис. 61) выберите страну местоположения защищаемого сервера в списке **Расположение** (подробнее о параметре читайте в п. A.5.5 на стр. 432).

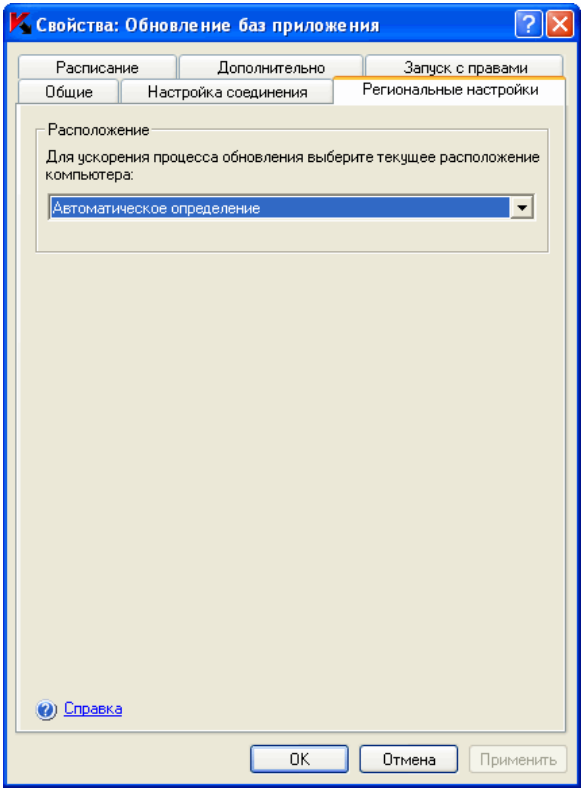

Рисунок 61. Диалоговое окно **Свойства задачи**, закладка **Региональные настройки**

8. После того как вы настроите нужные параметры, нажмите на кнопку **ОК**, чтобы сохранить изменения.

10.5.2. Настройка параметров задачи *Обновление модулей приложения*

*Чтобы настроить параметры задачи **Обновление модулей приложения**:*

1. В дереве консоли выберите узел **Обновление**.
2. Откройте контекстное меню на задаче **Обновление модулей приложения** и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: Обновление модулей приложения** укажите источник обновления и параметры соединения с ним (см. инструкцию в п. 10.5.1 на стр. 158).
4. На закладке **Общие** (см. рис. 62) выберите, копировать и устанавливать обновления или только проверять их наличие (подробнее о параметре см. A.5.6.1 на стр. 433).

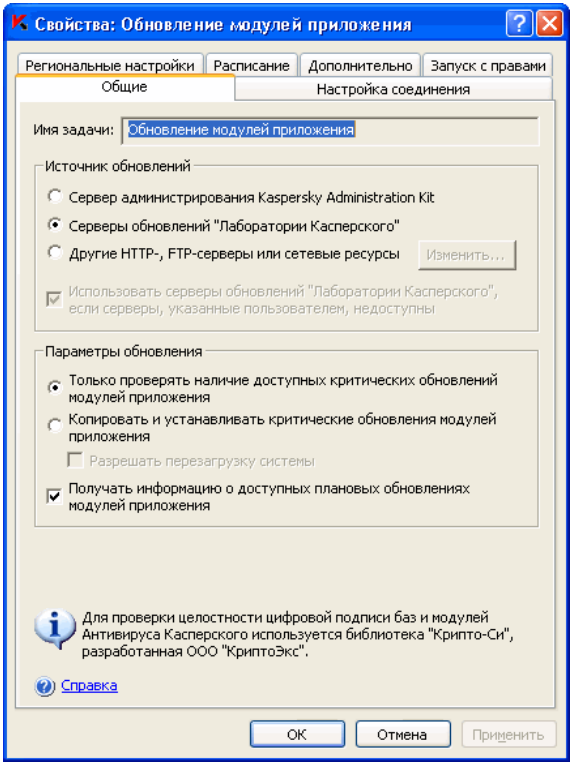

Рисунок 62. Диалоговое окно **Свойства: Обновление модулей приложения**, закладка **Общие**

5. Чтобы после завершения задачи Антивирус автоматически запускал перезагрузку сервера, если она потребуется для применения установленных программных модулей, установите флажок **Разрешать перезагрузку системы**.

6. Если вы хотите получать информацию о выходе плановых обновлений модулей Антивируса, установите флажок **Получать информацию о доступных плановых обновлениях модулей приложения**.

   «Лаборатория Касперского» не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете сами загружать их с веб-сайта «Лаборатории Касперского». Вы можете настроить уведомление администратора о событии *Доступны плановые обновления модулей Антивируса*, в котором будет содержаться адрес страницы нашего сайта, с которой вы

сможете загрузить плановые обновления (подробнее о настройке уведомлений читайте в п. 15.2 на стр. 237).

7. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

10.5.3. Настройка параметров задачи *Копирование обновлений*

*Чтобы настроить параметры задачи **Копирование обновлений**:*

1. В дереве консоли выберите узел **Обновление**.
2. Откройте контекстное меню на задаче **Копирование обновлений** и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: Копирование обновлений** (см. рис. 63) укажите источник обновления и параметры соединения с ним (см. инструкцию в п. 10.5.1 на стр. 158).

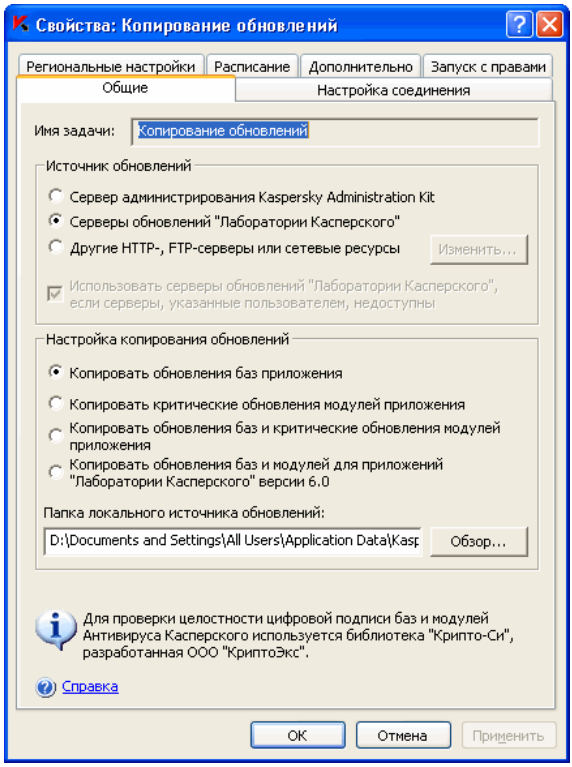

Рисунок 63. Диалоговое окно **Свойства: Копирование обновлений**, закладка **Общие**

4. На закладке **Общие** укажите состав обновлений, которые будут скопированы в указанную папку (подробнее о параметре читайте в п. A.5.7.1 на стр. 435).
5. Укажите локальную или сетевую папку, в которой Антивирус сохранит загруженные обновления (подробнее о параметре читайте в п. A.5.7.2 на стр. 437).
6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

10.6. Статистика задач обновления

Пока выполняется задача обновления, вы можете просматривать в реальном времени информацию об объеме данных, полученных с момента запуска задачи по текущий момент, – *статистику задачи*.

Информация в диалоговом окне **Статистика** будет доступна, если вы приостановите задачу. После завершения или остановки задачи вы сможете просмотреть эту информацию в подробном отчете о событиях в задаче (см. п. 13.2.4 на стр. 209).

Чтобы просмотреть статистику задачи обновления:

1. В дереве консоли разверните узел **Обновление**.
2. Откройте контекстное меню на нужной задаче обновления и выберите команду **Просмотреть статистику**.

В диалоговом окне **Статус выполнения задачи** задач **Обновление баз приложения** и **Копирование обновлений** отображается объем данных, загруженных Антивирусом на текущий момент (**Полученные данные**).

В диалоговом окне **Статус выполнения задачи Обновление модулей приложения** отображается следующая информация:

Поле	Описание
Полученные данные	Общий объем полученных данных
Доступно критических обновлений	Количество критических обновлений, доступных для установки
Доступно плановых обновлений	Количество плановых обновлений, доступных для установки
Ошибок применения обновлений	Если значение этого поля отличается от нуля, обновление не было применено. Вы можете просмотреть название обновления, при применении которого возникла ошибка, в подробном отчете о выполнении задачи.

10.7. Откат обновления баз Антивируса

Антивирус, перед тем, как применять обновления баз, создает резервные копии баз, используемых ранее. Если обновление прервалось или завершилось с ошибкой, Антивирус автоматически возвращается к использованию баз с предыдущими установленными обновлениями.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу **Откат обновления баз**.

10.8. Откат обновления программных модулей

Перед тем как применять обновления программных модулей, Антивирус создает резервные копии модулей, используемых в текущий момент. Если обновление модулей прервалось или завершилось с ошибкой, Антивирус автоматически возвращается к использованию модулей с последними установленными обновлениями.

Вы можете *вручную откатить программные модули* до предыдущих установленных обновлений.

Чтобы откатить программные модули, используйте компонент панели управления Microsoft Windows ***Установка и удаление программ****.*

ГЛАВА 11. ИЗОЛИРОВАНИЕ ПОДОЗРИТЕЛЬНЫХ ОБЪЕКТОВ. ИСПОЛЬЗОВАНИЕ КАРАНТИНА

В этой главе содержится следующая информация:

- об изолировании подозрительных объектов (см. п. 11.1 на стр. 169);
- просмотр объектов на карантине, сортировка и фильтрация объектов (см. п. 11.2 на стр. 170);
- проверка объектов на карантине (по требованию или автоматически, после каждого обновления баз) (см. п. 11.3 на стр. 175);
- восстановление объектов из карантина (см. п. 11.4 на стр. 177);
- помещение объектов на карантин вручную (см. п. 11.5 на стр. 181);
- удаление объектов из карантина (см. п. 11.6 на стр. 182);
- отправка подозрительных объектов из карантина на исследование в «Лабораторию Касперского» (см. п. 11.7 на стр. 183);
- настройка параметров карантина (см. п. 11.8 на стр. 185);
- статистика карантина (см. п. 11.9 на стр. 187).

Параметры карантина описаны в п. A.6 на стр. 438.

11.1. Об изолировании подозрительных объектов

Антивирус изолирует объекты, которые он признает подозрительными, помещая их *на карантин* – перенося из исходного местоположения в специальную папку, в которой в целях безопасности они хранятся в зашифрован-

ном виде (подробнее о том, как Антивирус признает объекты подозрительными, читайте в п. 1.1.3 на стр. 20).

11.2. Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в узле **Карантин** консоли Антивируса.

Чтобы просмотреть объекты на карантине, в дереве консоли выберите узел ***Карантин*** *(см. рис. 64).*

Чтобы найти нужный объект в списке объектов на карантине, вы можете отсортировать объекты (см. п. 11.2.1 на стр. 173) или отфильтровать их (см. п. 11.2.2 на стр. 173).

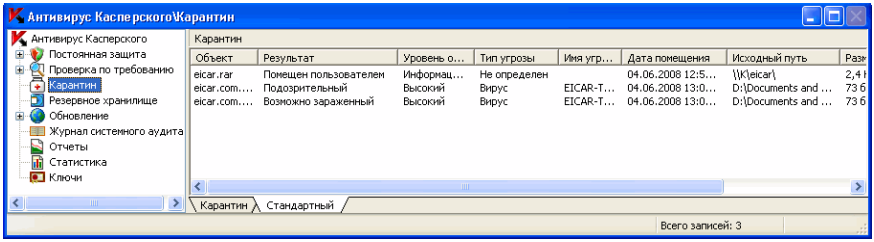

Рисунок 64. Информация об объектах на карантине в узле **Карантин**

В панели результатов отображается следующая информация о каждом объекте на карантине:

Таблица 7. Информация об объектах на карантине

Поле	Описание
Объект	Имя объекта, помещенного на карантин
Результат	Статус объекта на карантине; может иметь следующие значения: • **Предупреждение**. Объект признан подозрительным с использованием эвристического анализатора; • **Подозрительный**. Объект признан подозрительным – обнаружено частичное совпадение участка кода объекта с участком кода известной угрозы; • **Зараженный**. Объект признан зараженным – обнаружено полное совпадение участка кода объекта с участком кода известной угрозы; • **Ложное срабатывание**. Антивирус поместил объект на карантин как подозрительный или вы поместили объект на карантин вручную, но при проверке карантина использованием обновленных баз Антивирус признал объект незараженным. • **Вылечен**. Антивирус поместил объект на карантин как подозрительный или вы поместили объект на карантин вручную, но при проверке карантина с применением обновленных баз Антивирус признал объект зараженным и вылечил его. Вы можете безопасно восстановить объект; • **Помещен пользователем**. Объект помещен на карантин пользователем.

Поле	Описание
Уровень опасности	Уровень опасности показывает, насколько объект опасен для сервера Уровень опасности зависит от типа угрозы в объекте и может принимать следующие значения (подробнее о типах угроз читайте в п. 1.1.2 на стр. 16): • **Высокий**. Объект может содержать угрозу типа *сетевые черви*, *классические вирусы*, *троянские программы* или угрозу неопределенного типа (этот тип включает новые вирусы, на текущий момент не причисленные ни к одному из известных типов); • **Средний**. Объект может содержать угрозу типа *прочие вредоносные программы*, *программы-рекламы* или *программы порнографического содержания*; • **Низкий**. Объект может содержать угрозу типа *потенциально опасные программы*; • **Информационный**. Объект помещен на карантин пользователем.
Тип угрозы	Тип угрозы по классификации «Лаборатории Касперского»; входит в полное название угрозы, которое возвращает Антивирус, признав объект подозрительным или зараженным
Имя угрозы	Имя угрозы по классификации «Лаборатории Касперского», входит в полное название угрозы в объекте, которое возвращает Антивирус, признав объект подозрительным или зараженным Вы можете просмотреть полное название угрозы, обнаруженной в объекте, в подробном отчете о выполнении задачи (узел **Отчеты**).
Дата помещения	Дата помещения объекта на карантин
Исходный путь	Полный путь к исходному местоположению объекта, например, к папке, из которой объект был перенесен в папку карантина, файлу в составе архива или *pst*-файлу в почтовой базе
Размер	Размер объекта

Поле	Описание
Имя пользователя	В этом столбце отображаются следующие данные: • если объект был изолирован Антивирусом в задаче **Постоянная защита файлов** – имя учетной записи, с правами которой к объекту обращалось приложение, когда Антивирус перехватил этот объект; • если объект был изолирован Антивирусом в задаче проверки по требованию – имя учетной записи, с правами которой задача выполнялась; • если объект был помещен на карантин пользователем вручную – имя учетной записи этого пользователя.

11.2.1. Сортировка объектов на карантине

По умолчанию объекты в списке объектов на карантине отсортированы по дате помещения в обратном хронологическом порядке. Чтобы найти нужный объект, вы можете отсортировать объекты по содержимому столбцов с информацией об объектах. Результат сортировки сохранится, если вы покинете и снова откроете узел **Карантин** или если вы закроете консоль Антивируса с сохранением в *msc*-файл и снова откроете ее из этого файла.

Чтобы отсортировать объекты:

1. В дереве консоли выберите узел **Карантин**.
2. В панели результатов щелкните на заголовке столбца, по содержимому которого вы хотите отсортировать объекты в списке.

11.2.2. Фильтрация объектов в карантине

Чтобы найти нужный объект на карантине, вы можете отфильтровать объеты в списке – отобразить только те объекты, которые удовлетворяют заданным вами критериям фильтрации (фильтрам). Результат фильтрации сохранится, если вы покинете и снова откроете узел **Карантин** или если вы закроете консоль Антивируса с сохранением в *msc*-файл и снова откроете ее из этого файла.

Чтобы задать один или несколько фильтров:

1. В дереве консоли откройте контекстное меню на узле **Карантин** и выберите команду **Фильтр**.

   Откроется диалоговое окно **Параметры фильтра** (см. рис. 65).

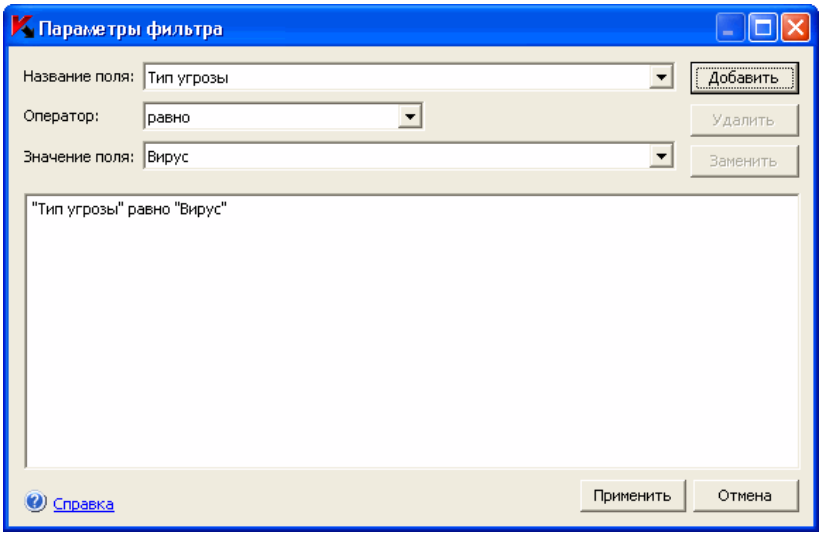

Рисунок 65. Диалоговое окно **Параметры фильтра**

2. Чтобы добавить фильтр:

   а) В списке **Название поля** выберите поле, с которым будет сравниваться значение фильтра.

   б) В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в списке **Название поля**.

   в) В поле **Значение поля** введите или выберите в списке значение фильтра.

   г) Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого фильтра, который вы хотите добавить. Если вы зададите несколько фильтров, то они объединятся по логическому «**И**».

- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.

- Чтобы отредактировать фильтр, выберите фильтр в списке в диалоговом окне **Параметры фильтра**, затем измените нужные значения в полях **Название поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить**.

3. После того как вы добавите все фильтры, нажмите на кнопку **Применить**.

*Чтобы снова отобразить все объекты в списке объектов на карантине, в дереве консоли откройте контекстное меню на узле **Карантин** и выберите команду **Снять фильтр**.*

11.3. Проверка объектов на карантине. Параметры задачи *Проверка объектов на карантине*

По умолчанию после каждого обновления баз Антивирус выполняет системную задачу **Проверка объектов на карантине**. Параметры задачи приводятся в таблице 8. Вы не можете их изменять.

Вы можете изменять расписание задачи **Проверка объектов на карантине** или запускать ее вручную.

Проверив объекты на карантине после обновления баз, Антивирус может признать некоторые из них незараженными: статус таких объектов изменится на **Ложное срабатывание**. Другие объекты Антивирус может признать зараженными и выполнить над ними действия, указанные параметрами задачи проверки по требованию **Проверка объектов на карантине**: **лечить, если невозможно, удалить**.

Таблица 8. Параметры задачи **Проверка объектов на карантине**

Параметр задачи Проверка объектов на карантине	**Значение**
Область проверки	Папка карантина
Параметры безопасности	Единые для всей области проверки; их значения приводятся в таблице 9.

Таблица 9. Параметры безопасности в задаче **Проверка объектов на карантине**

Параметр безопасности	Значение
Проверяемые объекты (см. п. A.3.2 на стр. 400)	Все объекты
Проверка только новых и измененных объектов (см. п. A.3.3 на стр. 402)	Выключена
Действие над зараженными объектами (см. п. A.3.5 на стр. 404)	Лечить, удалять, если лечение невозможно
Действие над подозрительными объектами (см. п. A.3.6 на стр. 407)	Пропускать
Исключение объектов (см. п. A.3.8 на стр. 411)	Нет
Исключение угроз (см. п. A.3.9 на стр. 412)	Нет
Макс. продолжительность проверки объекта (см. п. A.3.10 на стр. 414)	Не задана
Макс. размер проверяемого объекта (см. п. A.3.11 на стр. 415)	Не задан
Проверка дополнительных потоков файловой системы (NTFS) (см. п. A.3.2 на стр. 400)	Включена
Проверка загрузочных секторов (см. п. A.3.2 на стр. 400)	Выключена
Применение технологии ICheck-er (см. п. A.3.12 на 416)	Выключено
Применение технологии ISwift (см. п. A.3.13 на стр. 417)	Выключено

Параметр безопасности	Значение
Проверка составных объектов (см. п. A.3.4 на стр. 403)	• Архивы* • SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* * Проверка только новых и измененных объектов выключена.

11.4. Восстановление объектов из карантина

Антивирус помещает подозрительные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемый сервер от их возможного вредоносного действия.

Вы можете восстановить любой объект из карантина. Это может потребоваться в следующих случаях:

- если после проверки карантина с применением обновленных баз статус объекта изменился на **Ложное срабатывание** или **Вылечен**;
- если вы считаете объект безопасным для сервера и хотите его использовать. Чтобы Антивирус не изолировал этот объект при последующих проверках, вы можете исключить объект из обработки в задаче **Постоянная защита файлов** и задачах проверки по требованию. Для этого укажите объект в качестве значения параметра безопасности **Исключение объектов** (по имени файла) (см. п. A.3.8 на стр. 411) или **Исключение угроз** (см. п. A.3.9 на стр. 412) в этих задачах.

При восстановлении объекта вы можете выбрать, где будет сохранен восстановленный объект: в исходном местоположении (по умолчанию), в специальной папке для восстановления на защищаемом сервере или в указанной вами папке на компьютере, на котором установлена консоль Антивируса, или на другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом сервере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами карантина (см. п. 11.8 на стр. 185).

Внимание!

Восстановление объектов из карантина может привести к заражению компьютера.

Примечание

Если объект, помещенный на карантин, входит в составной объект (например, в архив), Антивирус не включает его снова составной объект при восстановлении, а сохраняет отдельно, в указанной папке.

Вы можете восстановить объект, сохранив его копию в папке карантина, чтобы использовать ее в дальнейшем, например, чтобы еще раз проверить объект после обновления баз.

Вы можете восстановить один или несколько объектов.

Чтобы восстановить объекты из карантина:

1. В дереве консоли выберите узел **Карантин**.
2. В панели результатов выполните одно из следующих действий:
   - чтобы восстановить один объект, откройте контекстное меню на объекте, который вы хотите восстановить, и выберите команду **Восстановить**;
   - чтобы восстановить несколько объектов, выберите нужные объекты, используя клавишу **<Ctrl>** или клавишу **<Shift>**, затем откройте контекстное меню на одном из выбранных объектов и выберите команду **Восстановить**.

   Откроется диалоговое окно **Восстановление объекта** (см. рис. 66).

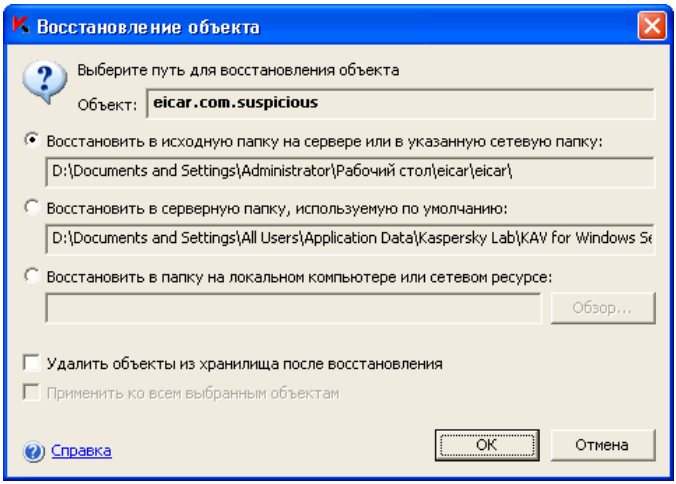

Рисунок 66. Диалоговое окно **Восстановление объекта**

3. В диалоговом окне **Восстановление объекта** для каждого из выбранных объектов укажите папку, в которой будет сохранен восстановленный объект (имя объекта отображается в поле **Объект** в верхней части диалогового окна; если вы выбрали несколько объектов, то отображается имя первого объекта в списке выбранных).

   Выполните одно из следующих действий:

   - чтобы восстановить объект в исходное местоположение, выберите **Восстановить в исходную папку на сервере или в указанную сетевую папку**;
   - чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления в параметрах карантина (см. п. A.6.4 на стр. 441), выберите **Восстановить в серверную папку для восстановления по умолчанию**;
   - чтобы сохранить объект в другую папку на компьютере, на котором установлена консоль Антивируса, или в сетевую папку, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.

4. Если вы хотите сохранить копию объекта в папке карантина после его восстановления, снимите флажок **Удалять объекты из карантина после восстановления**.

5. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное вами местоположение: если вы выбрали **Восстановить в исходную папку на сервере или указанную сетевую папку**, каждый из объектов будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в серверную папку для восстановления по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе** – все объекты будут сохранены в одну указанную папку.

6. Нажмите на кнопку **ОК**.

   Антивирус начнет восстанавливать первый из выбранных вами объектов.

7. Если объект с таким именем уже существует в указанном местоположении, то откроется диалоговое окно **Объект с таким именем существует** (см. рис. 67).

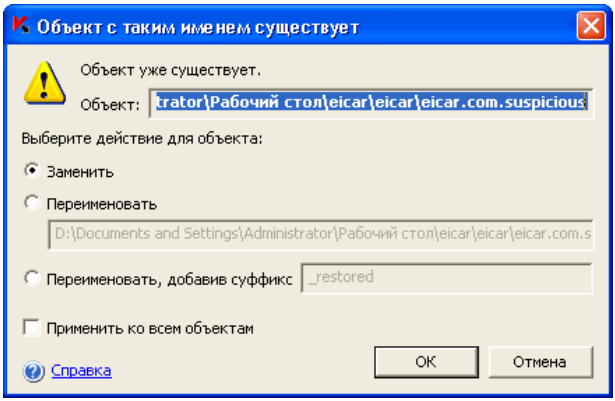

Рисунок 67. Диалоговое окно **Объект с таким именем существует**

   a) Выберите одно из следующих действий Антивируса:

      - **Заменить**, чтобы сохранить восстановленный объект вместо существующего;
      - **Переименовать**, чтобы сохранить восстановленный объект под другим именем. В поле ввода введите новое имя файла объекта и полный путь к нему;

- **Переименовать, добавив суффикс**, чтобы переименовать объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

б) Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие **Заменить** или **Переименовать, добавив суффикс** к остальным выбранным объектам, установите флажок **Применить ко всем объектам**. (Если вы указали **Переименовать**, то флажок **Применить ко всем объектам** будет недоступен.)

в) Нажмите на кнопку **ОК**.

Объект будет восстановлен; информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы не выбрали вариант **Применить ко всем выбранным объектам** в диалоговом окне **Восстановление объекта**, то диалоговое окно **Восстановление объекта** откроется снова. В нем вы сможете указать местоположение, в которое будет восстановлен следующий выбранный объект (см. шаг 3 этой инструкции).

11.5. Помещение файлов на карантин

Вы можете вручную помещать файлы на карантин.

Чтобы поместить файлы на карантин:

1. В дереве консоли откройте контекстное меню на узле **Карантин** и выберите команду **Добавить**.
2. В диалоговом окне **Открыть** выберите файлы на диске, которые вы хотите поместить на карантин, и нажмите на кнопку **ОК**.

> **Примечание**
>
> Если файлы, которые вы хотите поместить на карантин, хранятся в одной папке, то в диалоговом окне **Открыть** вы можете выбрать несколько файлов, используя клавишу **<Ctrl>** или клавишу **<Shift>**.

Антивирус поместит выбранный файл (файлы) на карантин.

3. В диалоговом окне с названием первого выбранного файла выполните следующее действие (если вы хотите применить действие ко

всем выбранным файлам, установите флажок **Применить к всем выбранным объектам**):

- чтобы сохранить файл в исходном местоположении, нажмите на кнопку **Сохранить**;
- чтобы удалить файл из исходного местоположения, нажмите на кнопку **Удалить**.

11.6. Удаление объектов из карантина

Согласно параметрам задачи **Проверка объектов на карантине** (см. п. 11.3 на стр. 175), Антивирус автоматически удаляет из папки карантина объекты, статус которых при проверке карантина с использованием обновленных баз изменился на **Зараженный** и которые Антивирусу не удалось вылечить. Остальные объекты Антивирус не удаляет.

Вы можете вручную удалить из карантина один или несколько объектов.

Чтобы удалить из карантина один или несколько объектов:

1. В дереве консоли выберите узел **Карантин**.
2. Выполните одно из следующих действий:
   - чтобы удалить один объект, откройте контекстное меню на объекте, который вы хотите удалить, и выберите команду **Удалить**;
   - чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавишу **<Ctrl>** или клавишу **<Shift>**, затем откройте контекстное меню на любом из выбранных объектов и выберите команду **Удалить**.
3. В диалоговом окне **Подтверждение** нажмите на кнопку **Да**, чтобы подтвердить операцию.

11.7. Отправка подозрительных объектов на исследование в «Лабораторию Касперского»

Если поведение какого-нибудь файла дает вам основание подозревать в нем наличие угрозы, а Антивирус признает этот файл незараженным, то, возможно, вы встретились с новой, неизвестной угрозой, алгоритм лечения которой еще не добавлен в базы. Вы можете отправить этот файл на исследование в «Лабораторию Касперского». Вирусные аналитики «Лаборатории Касперского» проанализируют его и, если обнаружат в нем новую угрозу, добавят идентифицирующую ее запись и алгоритм лечения в базы. Возможно, когда вы вновь проверите объект после обновления баз, Антивирус признает его зараженным и ему удастся его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Вы можете отправлять на исследование только файлы из карантина. В нем они хранятся в зашифрованном виде, и при пересылке не будут удалены антивирусным приложением, установленном на почтовом сервере.

Вы можете отправить на исследование файл на карантине, которому Антивирус присвоил статус *Подозрительный* или *Предупреждение*. Вы не можете отправить на исследование файл на карантине, которому Антивирус присвоил статус *Зараженный*. Подробнее о том, как Антивирус находит угрозы в объектах, читайте в п. 1.1.3 на стр. 20.

Примечание

Вы не можете отправить объект из карантина на исследование в «Лабораторию Касперского» после окончания срока действия ключа.

Чтобы отправить файл на исследование в «Лабораторию Касперского»:

1. Если файл не находится на карантине, предварительно поместите его на карантин (см. п. 11.5 на стр. 181).
2. В узле **Карантин**, в списке объектов на карантине, откройте контекстное меню на файле, который вы хотите отправить на исследование в «Лабораторию Касперского», и выберите команду **Отправить в лабораторию**.
3. Если на компьютере, на котором установлена консоль Антивируса, настроен почтовый клиент, будет создано новое электронное сообщение. Просмотрите его, а затем нажмите на кнопку **Отправить**.

Поле **Получатель** сообщения содержит электронный адрес «Лаборатории Касперского» newvirus@kaspersky.com. Поле **Тема** содержит текст «Объект карантина».

Тело сообщения содержит текст «Файл будет отправлен в «Лабораторию Касперского» для исследования». В тело сообщения вы можете включить любую дополнительную информацию о файле: почему он показался вам подозрительным, как он себя ведет или как влияет на систему.

В сообщение вложен архив *<имя объекта>.cab*. Он содержит файл *<uuid>.klq* с зашифрованным объектом, файл *<uuid>.txt* с информацией, собранной Антивирусом об объекте, а также файл *Sysinfo.txt*, который содержит следующую информацию об Антивирусе и операционной системе на сервере:

- название и версию операционной системы;
- название и версию Антивируса;
- дату выпуска последних установленных обновлений баз;
- серийный номер активного ключа.

Эта информация нужна вирусным аналитикам «Лаборатории Касперского», чтобы быстрее и эффективнее проанализировать файл. Однако, если вы не хотите передавать ее, вы можете удалить файл *Sysinfo.txt* из архива.

4. Если почтовый клиент не настроен на компьютере, на котором установлена консоль Антивируса, откроется мастер подключения к интернету Microsoft Windows. Вы можете выполнить следующие действия:

   - следуя инструкциям мастера подключения к интернету создать новую учетную запись и отправить файл с этого компьютера;
   - покинуть мастер и сохранить выбранный зашифрованный объект в файл. Этот файл вы можете переслать в «Лабораторию Касперского» самостоятельно.

   Чтобы сохранить зашифрованный объект в файл:

   а) в открывшемся диалоговом окне с приглашением сохранить объект (см. рис. 68) нажмите на кнопку **ОК**;

   б) выберите папку на диске защищаемого сервера или сетевую папку, в которую вы хотите сохранить файл с объектом.

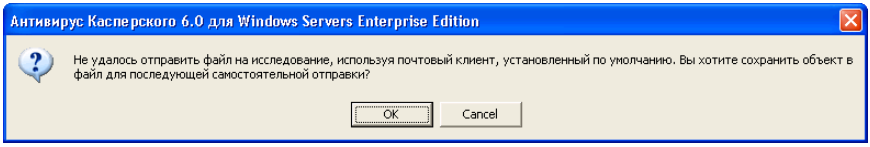

Рисунок 68. Диалоговое окно с приглашением сохранить объект на карантине в файл

11.8. Настройка параметров карантина

В этом разделе описана настройка параметров карантина. Новые значения параметров карантина применяются сразу после их сохранения.

Описание параметров карантина и их значения по умолчанию приводятся в п. A.6 на стр. 438.

Чтобы настроить параметры карантина:

1. В дереве консоли откройте контекстное меню на узле **Карантин** и выберите команду **Свойства** (см. рис. 69).

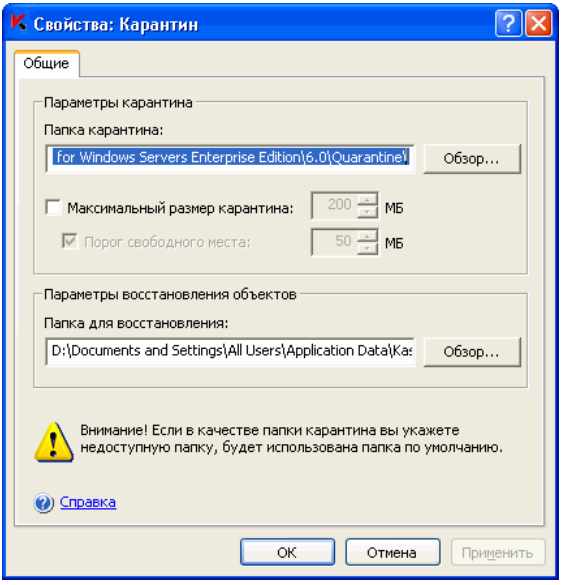

Рисунок 69. Диалоговое окно **Свойства: Карантин**

2. В диалоговом окне **Свойства: Карантин** настройте нужные параметры карантина в соответствии с вашими требованиями:

   - чтобы задать папку-местоположение карантина, отличную от папки по умолчанию, в поле **Папка карантина** выберите нужную папку на локальном диске защищаемого сервера или укажите ее имя и полный путь к ней (подробнее о параметре читайте в п. A.6.1 на стр. 438).

   - чтобы задать максимальный размер карантина, установите флажок **Максимальный размер карантина** и в поле ввода укажите нужное значение параметра в мегабайтах (см. п. A.6.2 на стр. 439);

   - чтобы задать минимальный размер свободного пространства в карантине, установите параметр **Максимальный размер карантина**, установите флажок **Порог свободного места** и в поле ввода укажите нужное значение параметра в мегабайтах (см. п. A.6.3 на стр. 440);

   - чтобы указать другую папку для восстановления, в группе параметров **Параметры восстановления объектов** выберите нужную папку на локальном диске защищаемого сервера или укажите ее имя и полный путь к ней (см. п. A.6.4 на стр. 441).

3. Нажмите на кнопку **ОК**.

11.9. Статистика карантина

Вы можете просматривать информацию о количестве объектов на карантине – *статистику карантина*.

Чтобы просмотреть статистику карантина, откройте контекстное меню на узле ***Карантин*** *в дереве консоли и выберите команду* ***Просмотреть статистику*** *(см. рис. 70).*

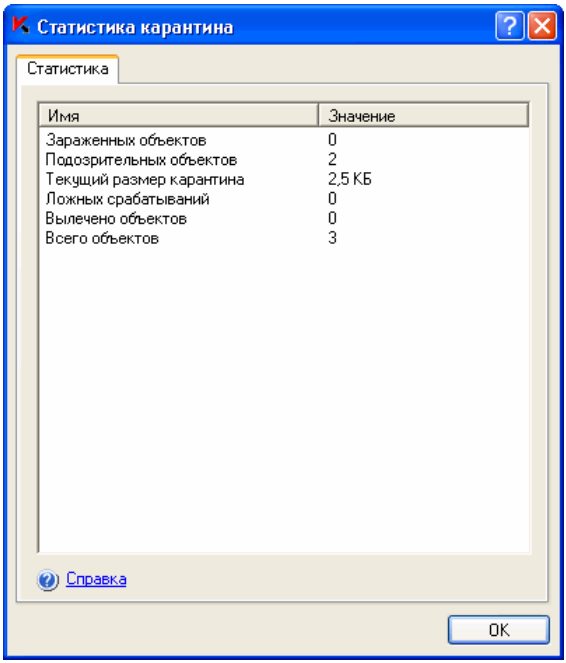

Рисунок 70. Диалоговое окно **Статистика карантина**

В диалоговом окне **Статистика карантина** отображается следующая информация о количестве объектов на карантине в текущий момент:

Поле	Описание
Зараженных объектов	Количество зараженных объектов: а) которые получили статус *Зараженный* после проверки карантина и которые Антивирусу не удалось вылечить или удалить, и б) которые Антивирус поместил на карантин согласно значению параметра **Действие в зависимости от типа угрозы**
Подозрительных объектов	Количество подозрительных объектов и потенциально опасных объектов Подробнее о том, как Антивирус находит угрозы в объектах, читайте в п. 1.1.3 на стр. 20.
Текущий размер карантина	Общий объем данных в папке карантина
Ложных срабатываний	Количество объектов, которые получили статус **Ложное срабатывание**, так как при проверке карантина с применением обновленных баз были признаны незараженными
Вылечено объектов	Количество объектов, которые после проверки карантина получили статус **Вылеченный**
Всего объектов	Общее количество объектов на карантине

ГЛАВА 12. РЕЗЕРВНОЕ КОПИРОВАНИЕ ОБЪЕКТОВ ПЕРЕД ЛЕЧЕНИЕМ / УДАЛЕНИЕМ. ИСПОЛЬЗОВАНИЕ РЕЗЕРВНОГО ХРАНИЛИЩА

В этой главе содержится следующая информация:

- о резервном копировании объектов перед лечением / удалением (см. п. 12.1 на стр. 189);
- просмотр файлов в резервном хранилище, сортировка и фильтрация файлов (см. п. 12.2 на стр. 190);
- восстановление файлов из резервного хранилища (см. п. 12.3 на стр. 195);
- удаление файлов из резервного хранилища (см. п. 12.4 на стр. 199);
- настройка параметров резервного хранилища (см. п. 12.5 на стр. 199);
- статистика резервного хранилища (см. п. 12.6 на стр. 201).

Параметры резервного хранилища описаны в п. A.7 на стр. 442.

12.1. О резервном копировании объектов перед лечением / удалением

Перед тем как выполнить лечение или удаление файла со статусом **Зараженный**, Антивирус сохраняет его зашифрованную копию в специальной папке – *резервном хранилище*.

Антивирус также сохраняет в резервном хранилище зашифрованные копии файлов со статусом **Подозрительный** или **Потенциально опасный**, если в параметрах безопасности задачи **Постоянная защита файлов** или задачах проверки по требованию вы выбрали **Удалять** в качестве действия над подозрительными объектами.

Если объект является частью составного объекта (например, входит в архив), то Антивирус сохраняет составной объект в резервном хранилище полностью.

Вы можете восстанавливать файлы из резервного хранилища, как в исходную папку, так и в другую папку на защищаемом сервере или другом компьютере в локальной сети. Вы можете восстановить файл из резервного хранилища, например, если исходный зараженный файл содержал важную информацию, но при лечении этого файла Антивирусу не удалось сохранить его целостность, и в результате информация в нем стала недоступной.

Внимание!

Восстановление файлов из резервного хранилища может привести к заражению компьютера.

12.2. Просмотр файлов в резервном хранилище

Вы можете просматривать файлы в папке резервного хранилища только через консоль Антивируса, в узле **Резервное хранилище**. Вы не можете просматривать их с помощью файловых менеджеров Microsoft Windows.

Чтобы просмотреть файлы в резервном хранилище, в дереве консоли выберите узел ***Резервное хранилище*** *(см. рис. 71).*

Чтобы найти нужный объект в списке, вы можете отсортировать объекты (см. п. 12.2.1 на стр. 192) или отфильтровать их (см. п. 12.2.2 на стр. 193).

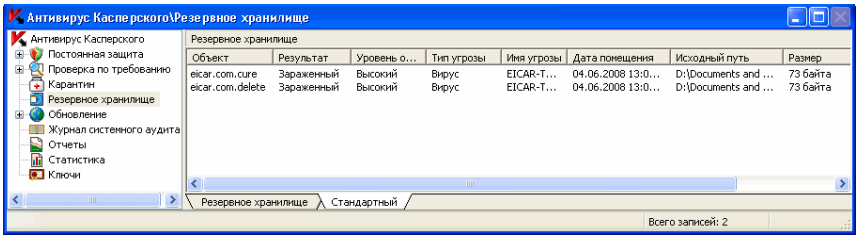

Рисунок 71. Информация о файлах в резервном хранилище в консоли Антивируса

В панели результатов отображается следующая информация о файле в резервном хранилище:

Поле	Описание
Объект	Имя файла, копия которого сохранена в резервном хранилище
Результат	Состояние файла с точки зрения наличия или отсутствия в нем угрозы: • **Зараженный**. Файл признан зараженным – обнаружено полное совпадение участка его кода с участком кода известной угрозы. • **Подозрительный**. Файл признан подозрительным – обнаружено частичное совпадение участка его кода с участком кода известной угрозы. • **Потенциально опасный**. Файл признан потенциально опасным эвристическим анализатором Антивируса. Подробнее о том, как Антивирус находит угрозы в объектах, читайте в п. 1.1.3 на стр. 20.
Уровень опасности	Уровень опасности показывает, насколько объект опасен для сервера. Уровень опасности зависит от типа угрозы в объекте и может принимать следующие значения: • **Высокий**. Файл может содержать угрозу типа *сетевые черви*, *классические вирусы*, *троянские программы* или угрозу неопределенного типа (этот тип включает новые вирусы, на текущий момент не причисленные ни к одному из известных типов); • **Средний**. Файл может содержать угрозу типа прочие *вредоносные программы*, *программы-рекламы* или *программы порнографического содержания*; • **Низкий**. Файл может содержать угрозу типа *потенциально опасные программы*. Подробнее об угрозах, которые обнаруживает Антивирус, читайте в п. 1.1.2 на стр. 16.

Поле	Описание
Тип угрозы	Тип угрозы по классификации «Лаборатории Касперского»; входит в полное название угрозы, которое возвращает Антивирус, признав файл зараженным или подозрительным. Вы можете просмотреть полное название угрозы в объекте в узле **Отчеты**, в подробном отчете о выполнении задачи.
Имя угрозы	Имя угрозы по классификации «Лаборатории Касперского»; входит в полное название угрозы, которое возвращает Антивирус, признав файл зараженным. Вы можете просмотреть полное название угрозы в объекте в узле **Отчеты**, в подробном отчете о выполнении задачи.
Дата помещения	Дата и время сохранения файла в папке резервного хранилища
Исходный путь	Полный путь к исходной папке – папке, в которой файл находился, перед тем как Антивирус сохранил его копию в резервном хранилище
Размер	Размер файла
Имя пользователя	В этом столбце отображаются следующие данные: • если Антивирус зарезервировал файл в задаче **Постоянная защита файлов** – имя учетной записи, с правами которой к файлу обращалось приложение, когда Антивирус перехватил файл; • если Антивирус зарезервировал файл в задаче проверки по требованию – имя учетной записи, с правами которой задача выполнялась.

О том, как настроить параметры резервного хранилища, см. п. 12.5 на стр. 199.

12.2.1. Сортировка файлов в резервном хранилище

По умолчанию файлы в резервном хранилище отсортированы по дате их сохранения в обратном хронологическом порядке. Чтобы найти нужный

файл, вы можете отсортировать файлы по содержимому любого столбца в панели результатов.

Результат сортировки сохранится, если вы покинете и снова откроете узел **Резервное хранилище** или если вы закроете консоль Антивируса с сохранением в *msc*-файл и снова откроете ее из этого файла.

Чтобы отсортировать файлы в резервном хранилище:

1. В дереве консоли выберите узел **Резервное хранилище**.
2. В списке файлов в резервном хранилище щелкните на заголовке столбца, по содержимому которого вы хотите отсортировать объекты.

12.2.2. Фильтрация файлов в резервном хранилище

Чтобы найти нужный файл в резервном хранилище, вы можете *отфильтровать* файлы – отобразить в узле **Резервное хранилище** только те файлы, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

Результат фильтрации сохранится, если вы покинете и снова откроете узел **Резервное хранилище** или если вы закроете консоль Антивируса с сохранением в *msc*-файл и снова откроете ее из этого файла

Чтобы отфильтровать файлы в резервном хранилище:

1. В дереве консоли откройте контекстное меню на узле **Резервное хранилище** и выберите команду **Фильтр**.

   Откроется диалоговое окно **Параметры фильтра** (см. рис. 72).

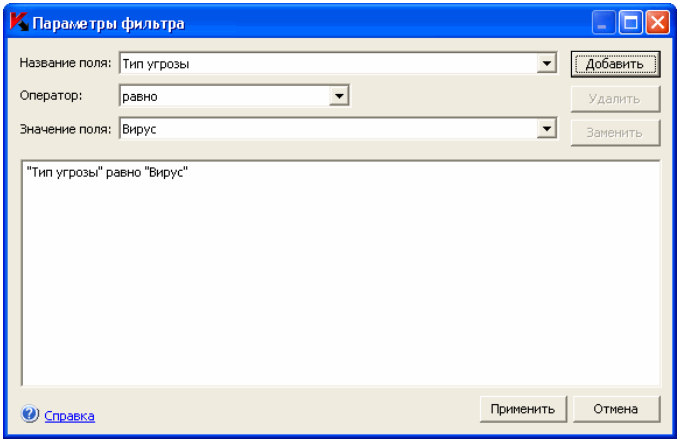

Рисунок 72. Диалоговое окно **Параметры фильтра**

2. Чтобы добавить фильтр, выполните следующие действия:

   а) В списке **Название поля** выберите поле, со значениями которого будет сравниваться указанное вами значение фильтра при отборе.

   б) В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в поле **Название поля**.

   в) В поле **Значение поля** введите или выберите значение фильтра.

   г) Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого фильтра, который вы хотите добавить. Если вы зададите несколько фильтров, то они объединятся по логическому «И».

- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.

- Чтобы отредактировать фильтр, выберите его в списке фильтров в диалоговом окне **Параметры фильтра** измените нужные значения в полях **Название поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить**.

3. После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке отобразятся только файлы, отобранные согласно заданным фильтрам.

Чтобы снова отобразить все файлы в списке файлов в резервном хранилище, в дереве консоли откройте контекстное меню на узле ***Резервное хранилище*** *и выберите команду* ***Снять фильтр****.*

12.3. Восстановление файлов из резервного хранилища

Антивирус хранит файлы в папке резервного хранилища в зашифрованном виде, чтобы предохранить защищаемый сервер от их возможного вредоносного действия.

Вы можете восстанавливать файлы из резервного хранилища.

Вам может потребоваться восстановить файл в следующих случаях:

- если исходный файл, который оказался зараженным, содержал важную информацию, при лечении файла Антивирусу не удалось сохранить его целостность, и в результате информация в файле стала недоступной;
- если вы считаете файл безопасным для сервера и хотите его использовать. Чтобы Антивирус не признавал файл зараженным или подозрительным при последующих проверках, вы можете исключить его из обработки в задаче **Постоянная защита файлов** и задачах проверки по требованию. Для этого укажите файл в качестве параметра **Исключение объекта** (см. п. A.3.8 на стр. 411) или **Исключение угроз** (см. п. A.3.9 на стр. 412).

Внимание!

Восстановление файлов из резервного хранилища может привести к заражению компьютера.

При восстановлении файла вы можете выбрать, куда он будет сохранен: в исходную папку (по умолчанию), в специальную папку для восстановленных объектов на защищаемом сервере или в указанную вами папку на компьютере, на котором установлена консоль Антивируса, или другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом сервере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами резервного хранилища (о том, как настроить их см. п. 12.5 на стр. 199).

По умолчанию, когда Антивирус восстанавливает файл, он удаляет его копию из резервного хранилища. Вы можете сохранить копию файла в резервном хранилище после его восстановления.

Чтобы восстановить файлы из резервного хранилища:

1. В дереве консоли выберите узел **Резервное хранилище**.
2. Выполните одно из следующих действий:
   - чтобы восстановить один файл, в списке файлов в резервном хранилище откройте контекстное меню на файле, который вы хотите восстановить, и выберите команду **Восстановить**.
   - чтобы восстановить несколько файлов, выберите нужные файлы в списке, используя клавишу **<Ctrl>** или клавишу **<Shift>**, затем откройте контекстное меню на одном из выбранных файлов и выберите команду **Восстановить**.
3. В диалоговом окне **Восстановление объекта** (см. рис. 73) укажите папку, в которой будет сохранен восстановленный файл.

   Название файла отображается в поле **Объект** в верхней части диалогового окна. Если вы выбрали несколько файлов, то отображается имя первого файла в списке выбранных.

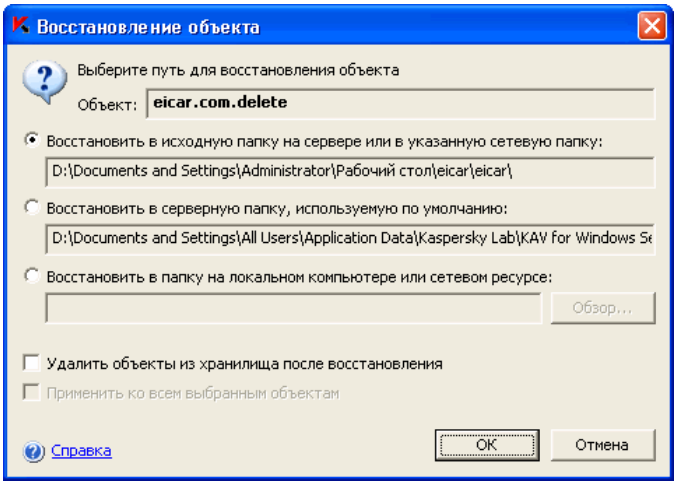

Рисунок 73. Диалоговое окно **Восстановление объекта**

Выполните одно из следующих действий:

- чтобы сохранить восстановленный файл на защищаемом сервере, выберите:

- **Восстановить в исходную папку на сервере или указанную сетевую папку**, если вы хотите восстановить файл в исходную папку;
- **Восстановить в серверную папку, используемую по умолчанию**, если вы хотите восстановить файл в папку, которую вы указали в качестве папки для восстановления в параметрах резервного хранилища (см. п. 12.5 на стр. 199);

- чтобы сохранить восстановленный файл в другую папку, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе** и выберите нужную папку (на компьютере, на котором установлена консоль Антивируса, или сетевую) или укажите путь к ней.

4. Если вы хотите сохранить копию файла в папке резервного хранилища после его восстановления, снимите флажок **Удалять объекты из хранилища после восстановления**.

5. Если вы выбрали несколько файлов для восстановления, то, чтобы применить указанные условия сохранения к остальным выбранным файлам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные файлы будут восстановлены и сохранены в указанную вами папку: если вы выбрали **Восстановить в исходную папку на сервере или в указанную сетевую папку**, каждый из файлов будет сохранен в свою исходную папку; если вы выбрали **Восстановить в серверную папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе**, все файлы будут сохранены в одну указанную папку.

6. Нажмите на кнопку **ОК**.

   Антивирус начнет восстанавливать первый из выбранных вами файлов.

7. Если файл с таким именем уже существует в указанной папке, то откроется диалоговое окно **Объект с таким именем существует** (см. рис. 74).

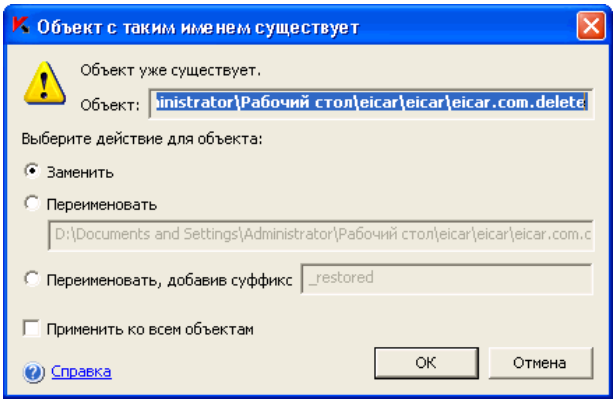

Рисунок 74. Диалоговое окно **Объект с таким именем существует**

Выполните следующие действия:

а) Выберите условие сохранения восстановленного файла:

- **Заменить**, чтобы сохранить восстановленный файл вместо существующего;
- **Переименовать**, чтобы сохранить восстановленный файл под другим именем. В поле ввода введите новое имя файла и полный путь к нему;
- **Переименовать, добавив суффикс**, чтобы переименовать файл, добавив к его имени суффикс. Введите суффикс в поле ввода.

б) Если вы хотите приименить выбранное действие **Заменить** или **Переименовать, добавив суффикс** к остальным выбранным файлам, установите флажок **Применить ко всем объектам**.

(Если вы указали **Переименовать**, то флажок **Применить ко всем объектам** будет недоступен.)

в) Нажмите на кнопку **ОК**.

Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы выбрали несколько файлов для восстановления и не выбрали вариант **Применить ко всем выбранным объектам** в диалоговом окне **Восстановление объекта**, то диалоговое окно **Восстановление объекта** откроется снова. В нем вы

сможете указать папку, в которой будет сохранен при восстановлении следующий выбранный файл (см. шаг 3 этой инструкции).

12.4. Удаление файлов из резервного хранилища

Чтобы удалить из резервного хранилища один или несколько файлов:

1. В дереве консоли выберите узел **Резервное хранилище**.
2. Выполните одно из следующих действий:
   - чтобы удалить один файл, в списке объектов откройте контекстное меню на файле, который вы хотите удалить, и выберите команду **Удалить**;
   - чтобы удалить несколько файлов, выберите нужные файлы в списке, используя клавишу **<Ctrl>** или клавишу **<Shift>**, затем откройте контекстное меню на любом из выбранных файлов и выберите команду **Удалить**.
3. В диалоговом окне **Подтверждение** нажмите на кнопку **Да**, чтобы подтвердить операцию. Выбранные файлы будут удалены.

12.5. Настройка параметров резервного хранилища

В этом разделе описано, как настраивать параметры резервного хранилища. Описание параметров резервного хранилища и их значения по умолчанию приводятся в п. A.7 на стр. 442.

Новые значения параметров резервного хранилища применяются сразу после их сохранения.

Чтобы настроить параметры резервного хранилища:

1. В дереве консоли откройте контекстное меню на узле **Резервное хранилище** и выберите команду **Свойства** (см. рис. 75).

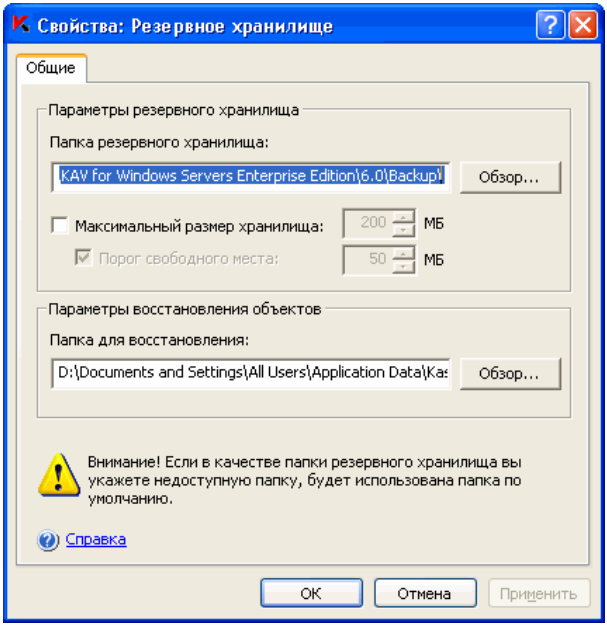

Рисунок 75. Диалоговое окно **Свойства: Резервное хранилище**

2. В диалоговом окне **Свойства: Резервное хранилище** выполните следующее:

   - чтобы задать папку-местоположение резервного хранилища, в поле **Папка резервного хранилища**, выберите нужную папку на локальном диске защищаемого сервера или введите полный путь к ней (подробнее о параметре читайте в п. A.7.1 на стр. 442);
   - чтобы задать максимальный размер резервного хранилища, установите флажок **Максимальный размер хранилища** и в поле ввода укажите нужное значение параметра в мегабайтах (см. п. A.7.2 на стр. 444);
   - чтобы задать порог свободного места в резервном хранилище, установите параметр **Максимальный размер хранилища**, установите флажок **Порог свободного места** и укажите минимальный размер свободного места в папке резервного хранилища в мегабайтах (см. п. A.7.3 на стр. 445).
   - чтобы задать папку для восстановления объектов, в группе параметров **Параметры восстановления объектов** выберите

нужную папку на локальном диске защищаемого сервера или в поле **Папка для восстановления** введите имя папки и полный путь к ней (см. п. A.7.4 на стр. 446).

3. Нажмите на кнопку **ОК**.

12.6. Статистика резервного хранилища

Вы можете просматривать информацию о состоянии резервного хранилища в текущий момент – *статистику резервного хранилища*.

Чтобы просмотреть статистику резервного хранилища, в дереве консоли откройте контекстное меню на узле ***Резервное хранилище*** *и выберите команду* ***Просмотреть статистику*** *(см. рис. 76).*

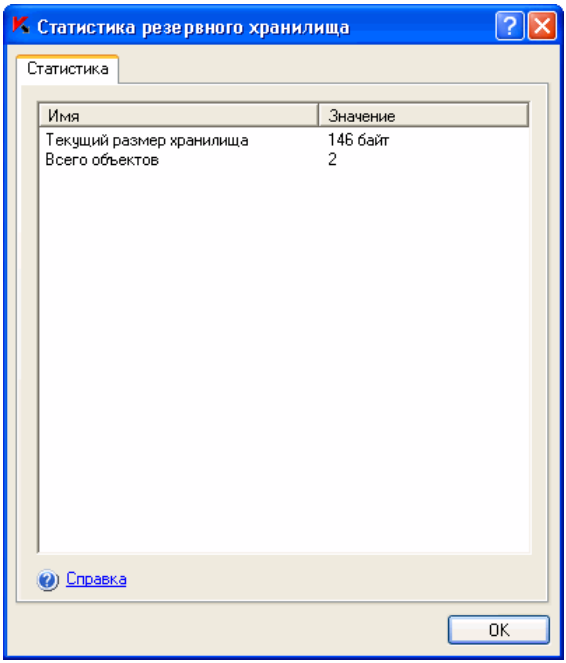

Рисунок 76. Диалоговое окно **Статистика резервного хранилища**

В диалоговом окне **Статистика резервного хранилища** отображается следующая информация о состоянии резервного хранилища в текущий момент:

Таблица 10. Статистика резервного хранилища

Поле	Описание
Текущий размер хранилища	Объем данных в папке в резервного хранилища
Всего объектов	Количество объектов в резервном хранилище в текущий момент

ГЛАВА 13. РЕГИСТРАЦИЯ СОБЫТИЙ

В этой главе содержится следующая информация:

- о способах регистрации событий в Антивирусе (см. п. 13.1 на стр. 203);
- отчеты о выполнении задач: просмотр, удаление, настройка (см. п. 13.2 на стр. 204);
- журнал системного аудита: просмотр, очистка (см. п. 13.3 на стр. 217);
- статистика Антивируса – информация о текущем состоянии Антивируса, его функциональных компонентов и выполняемых задач (см. п. 13.4 на стр. 221);
- журнал событий Антивируса в консоли MMC «Просмотр событий» Microsoft Windows (см. п. 13.5 на стр. 226).

13.1. Способы регистрации событий

События в Антивирусе делятся на связанные с обработкой объектов в задачах и связанные с управлением Антивирусом – к ним относят такие события, как запуск Антивируса, создание или удаление задач, запуск задач, изменение настроек задач и другие.

Антивирус регистрирует события следующим образом:

- создает *отчеты о выполнении задач*. Отчет о выполнении задачи содержит информацию о текущем состоянии задачи и событиях, которые возникли за время ее выполнения (см. п. 13.2 на стр. 204);
- ведет *журнал системного аудита*; в журнале регистрирует события, связанные с управлением Антивирусом (см. п. 13.3 на стр. 217);
- собирает *статистику* своей работы – информацию о текущем состоянии функциональных компонентов и выполняемых в текущий момент задачах (см. п. 13.4 на стр. 221);

- ведет ж*урнал событий* в консоли «Просмотр событий» Mocrosoft Windows; в журнале регистрирует события, важные для диагностики сбоев (см. п. 13.5 на стр. 226).

Если в работе Антивируса возникла проблема (например, Антивирус или отдельная задача завершается аварийно) и вы хотите диагностировать ее, вы можете создать *журнал трассировки* и *дампы памяти процессов Антивируса* и отправить файлы с этой информацией на анализ в Службу технической поддержки «Лаборатории Касперского». Подробнее о создании *журнала трассировки* и *файлов дампов памяти* читайте в п. 3.2 на стр. 46.

13.2. Отчеты о выполнении задач

В этом разделе содержится следующая информация:

- об отчетах о выполнении задач (см. п. 13.2.1 на стр. 204);
- просмотр сводных отчетов (см. п. 13.2.2 на стр. 205);
- сортировка сводных отчетов в списке (см. п. 13.2.3 на стр. 209);
- просмотр подробных отчетов в задачах (см. п. 13.2.4 на стр. 209);
- экспорт информации из подробного отчета в текстовый файл (см. п. 13.2.5 на стр. 214);
- удаление отчетов (см. п. 13.2.6 на стр. 214);
- изменение уровня детализации информации в отчетах о выполнении задач отдельных функциональных компонентов и журнале событий (см. п. 13.2.7 на стр. 215).

13.2.1. Об отчетах о выполнении задач

В узле **Отчеты** вы можете просматривать сводные и подробные отчеты о выполнении задач Антивируса. *Сводный отчет* – это строка с информацией о состоянии задачи и общем статусе обработанных объектов с точки зрения антивирусной безопасности. *Подробный отчет* содержит статистику выполнения задачи (информацию о количестве обработанных объектов), информацию о каждом объекте, обработанным Антивирусом с момента запуска задачи по текущий момент, а также параметры задачи.

По умолчанию отчеты хранятся ограниченное время. Из подробных отчетов о задачах, выполняемых в текущий момент, удаляются записи о событиях, созданные более 30 дней назад. Сводный отчет о задаче удаляется через 30 дней после ее завершения. С помощью параметров Антивируса вы можете изменить длительность хранения отчетов или отключить автоматиче-

ское удаление отчетов, чтобы хранить их неограниченное время (Глава 3 на стр. 46). Вы также можете вручную удалить выбранный отчет.

13.2.2. Просмотр сводных отчетов. Статусы сводных отчетов

Чтобы просмотреть сводный отчет о выполнении задачи:

1. В дереве консоли выберите узел **Отчеты** (см. рис. 77).

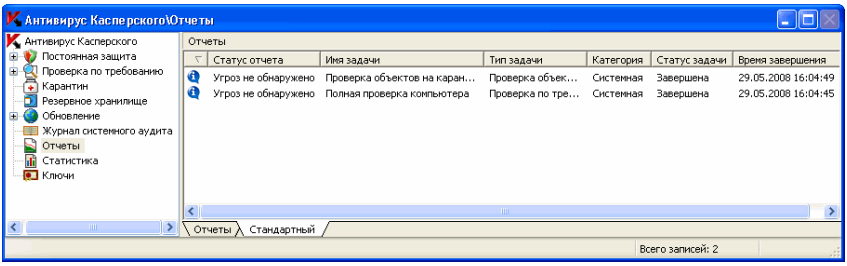

Рисунок 77. Список отчетов в панели результатов

2. В панели результатов найдите нужный отчет о задаче (чтобы быстро отыскать отчет в списке, вы можете отфильтровать записи или отсортировать их по содержимому любого из столбцов).

   О том, как просмотреть подробный отчет о выполнении задачи, см. п. 13.2.4 на стр. 209.

В отчете содержится следующая информация о выполнении задачи:

Таблица 11. Информация о выполнении задачи в отчете

Поле	Описание
Статус отчета	Сводная характеристика, полученная на основании статистики задачи; отражает общее состояние обработанных объектов с точки зрения антивирусной безопасности. По уровню важности статусы отчета делятся на *информационный*, *предупреждение*, и *критический*. В следующих таблицах описаны статусы отчета задач проверки по требованию и обновления.
Имя задачи	Имя задачи, отчет о которой вы просматриваете.

Поле	Описание
Тип задачи	Тип задачи, соответствует функциональному компоненту, в котором задача создана (постоянная защита файлов, проверка скриптов, проверка по требованию, обновление).
Категория	Категория задачи в Антивирусе: *системная*, *пользовательская* или *групповая*. Подробнее о категориях задач читайте в п. 5.1 на стр. 54.
Статус задачи	Состояние задачи в текущий момент: *Выполняется*, *Завершена*, *Приостановлена*, *Остановлена*, *Завершена с ошибкой*, *Запускается*, *Восстанавливается.*
Время завершения	Если к текущему моменту задача завершилась, то в этом столбце отображается дата и время ее завершения. Если в текущий момент задача выполняется, то это поле остается пустым.

Таблица 12. Статусы отчетов задач проверки по требованию

Уровень важности	Статус отчета	Описание статуса отчета
	Угроз не обнаружено	Антивирус проверил все объекты в выбранной области. Антивирус признал все проверенные объекты незараженными.
	Некоторые объекты не обработаны	Антивирус признал все проверенные объекты незараженными; один или несколько объектов были пропущены, например, были исключены из проверки параметрами безопасности или в момент обращения использовались другими программами. В момент обращения могут использоваться, например, системные файлы Microsoft Windows. Антивирус не проверяет их, и задача завершается со статусом *Некоторые объекты не были обработаны*.

Уровень важности	Статус отчета	Описание статуса отчета
	Обнаружены поврежденные объекты	Антивирус признал все проверенные объекты незараженными. Один или несколько объектов в выбранной области были пропущены: Антивирусу не удалось прочесть эти объекты, так как их формат искажен.
	Обнаружены подозрительные объекты	Антивирус признал один или несколько проверенных объектов подозрительными. Вы можете узнать, какие именно объекты оказались подозрительными, просмотрев подробный отчет о выполнении задачи (см. п. 13.2.4 на стр. 209).
	Обнаружены зараженные объекты	Антивирус обнаружил угрозы в одном или нескольких объектах. Вы можете узнать, какие именно объекты содержат угрозы, просмотрев подробный отчет о выполнении задачи (см. п. 13.2.4 на стр. 209).
	Ошибки обработки	Антивирус признал все проверенные объекты незараженными. Во время проверки одного или нескольких объектов возникла ошибка Антивируса. **Примечание** Объект, во время обработки которого возникла ошибка Антивируса, может содержать угрозу. Рекомендуется поместить такой объект на карантин и перепроверить его на карантине после обновления баз (см. п. 11.3 на стр. 175). Если ошибка повторится, обратитесь в Службу технической поддержки «Лаборатории Касперского». Подробнее о том, как обратиться в Службу технической поддержки, читайте в п. 1.2.3 на стр. 24.
	Критические ошибки	Задача завершилась аварийно. Вы можете посмотреть причину ошибки в подробном отчете о выполнении задачи.

Таблица 13. Статусы отчетов задач обновления баз и копирования обновлений

Уровень важности	Статус отчета	Описание статуса отчета
	Нет ошибок	Антивирус получил и успешно применил обновления.
	Критические ошибки	Возникла ошибка при получении обновлений или их применении. В подробном отчете о выполнении задачи вы можете просмотреть название неприменного обновления и причину ошибки.

Таблица 14. Статусы отчетов задач обновления модулей приложения

Уровень важности	Статус отчета	Описание статуса отчета
	Нет ошибок	Антивирус получил обновления и успешно применил их.
	Доступно критическое обновление	Опубликованы срочные обновления модулей Антивируса.
	Доступно плановое обновление	Опубликованы плановые обновления модулей Антивируса.
	Доступны критические и плановые обновления	Опубликованы и срочные, и плановые обновления модулей Антивируса.
	Выполняется установка полученных обновлений	Антивирус получил обновления и применяет их.
	Для завершения обновления требуется перезагрузка сервера	Перезагрузите сервер, чтобы применить обновления.
	Критические ошибки	Возникла ошибка при получении обновлений или их применении. В подробном отчете о выполнении задачи вы можете просмотреть название неприменного обновления и причину ошибки.

13.2.3. Сортировка отчетов

По умолчанию отчеты отображаются в списке в обратном хронологическом порядке. Вы можете сортировать отчеты по содержимому любого из столбцов. Результат сортировки сохранится, если вы покинете и снова выберете узел **Отчеты**, или, если вы закроете консоль Антивируса с сохранением в *msc*-файл и снова откроете ее из этого файла.

Чтобы отсортировать отчеты:

1. В дереве консоли выберите узел **Отчеты**.
2. В панели информации щелкните на заголовке столбца, по содержимому которого вы хотите отсортировать отчеты.

13.2.4. Просмотр подробного отчета о выполнении задачи

В подробном отчете о выполнении задачи вы можете просмотреть информацию обо всех событиях, возникших в задаче с момента ее запуска по текущий момент. Например, вы можете узнать, в каком из обработанных объектов была обнаружена угроза.

Чтобы просмотреть подробный отчет о выполнении задачи:

1. В дереве консоли выберите узел **Отчеты**.
2. В списке отчетов откройте контекстное меню на сводном отчете о задаче, подробный отчет о событиях в которой вы хотите просмотреть, выберите команду **Просмотреть отчет**.

Диалоговое окно **Подробный отчет** содержит закладку **События** с информацией о событиях в задаче, закладку **Статистика**, на которой отображается время запуска и завершения задачи и ее статистика, и закладку **Параметры** с параметрами задачи.

На закладке **События** содержится следующая информация о событиях в задаче (см. рис. 78):

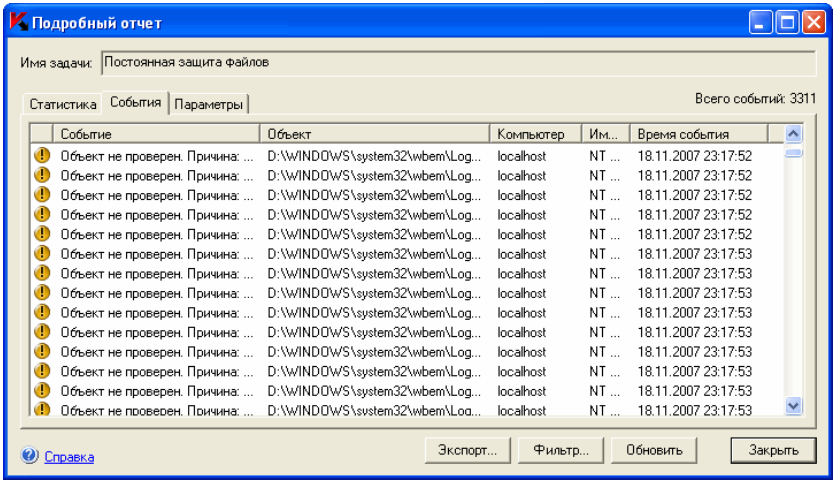

Рисунок 78. Пример подробного отчета о задаче **Постоянная защита файлов**

Поле	Описание
Уровень важности события	По уровню важности события в подробном отчете делятся на *информационные*, *важные* и *критические*.
Событие	Тип события и дополнительная информация о событии.
Объект	Имя обработанного объекта и путь к нему. В задаче **Проверка скриптов** в этом столбце также отображается идентификатор PID процесса, который выполнял перехваченный Антивирусом скрипт.
Время события	Дата и время возникновения события.

Подробный отчет о задаче **Постоянная защита файлов** содержит кроме указанных выше полей поля **Компьютер** и **Имя пользователя**; подробный отчет о задаче **Проверка скриптов** содержит поле **Имя пользователя**:

Поле	Описание
Компьютер	Имя компьютера, с которого приложение обратилось к объекту.

Имя пользователя	Имя пользователя, под учетной записью которого, приложение обратилось к объекту. Если к объекту обратилось приложение, которое работает под учетной записью **Локальная система** (**SYSTEM**), то в этом столбце содержится запись <домен><имя компьютера>$. В задаче **Постоянная защита файлов** Антивирус регистрирует в качестве имени компьютера значение localhost, а не сетевое имя защищаемого сервера, если к объекту обращается приложение, которое работает на защищаемом сервере.

*Чтобы просмотреть статистику задачи, в диалоговом окне **Подробный отчет** откройте закладку **Статистика** (см. рис. 79).*

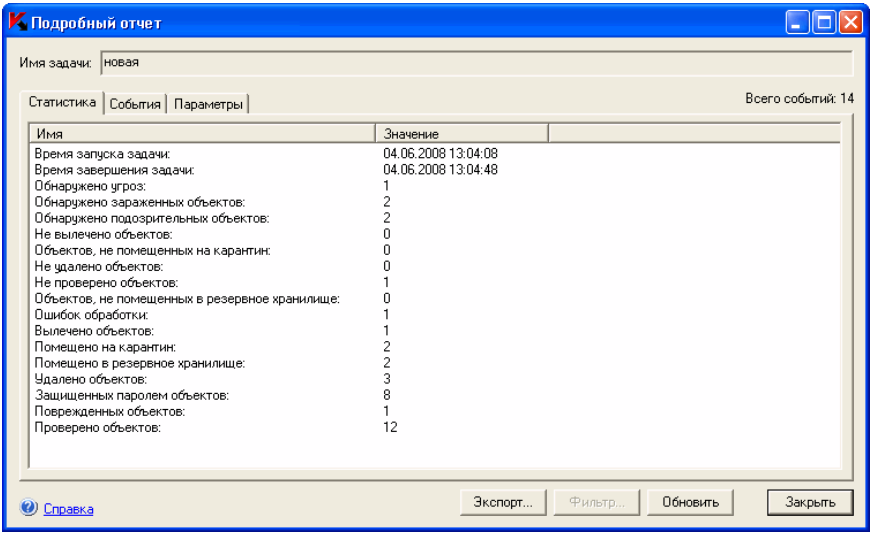

Рисунок 79. Диалоговое окно **Подробный отчет**, закладка **Статистика**

*Чтобы просмотреть параметры задачи, в диалоговом окне **Подробный отчет** откройте закладку **Параметры** (см. рис. 80).*

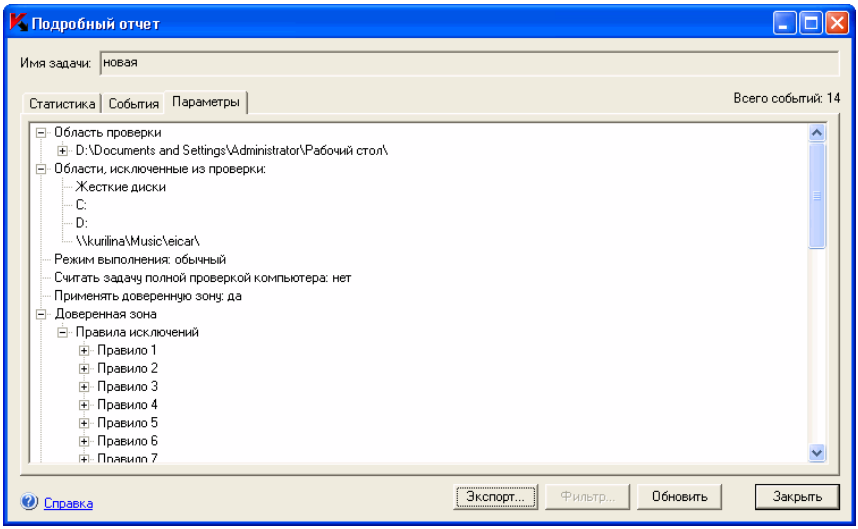

Рисунок 80. Диалоговое окно **Подробный отчет**, закладка **Параметры**

Просматривая подробный отчет, вы можете задать один или несколько фильтров, чтобы отыскать нужное событие на закладке **События**;

Чтобы задать один или несколько фильтров:

1. Нажмите на кнопку **Фильтр** в нижней части диалогового окна **Подробный отчет**. Откроется диалоговое окно **Параметры фильтра** (см. рис. 81).

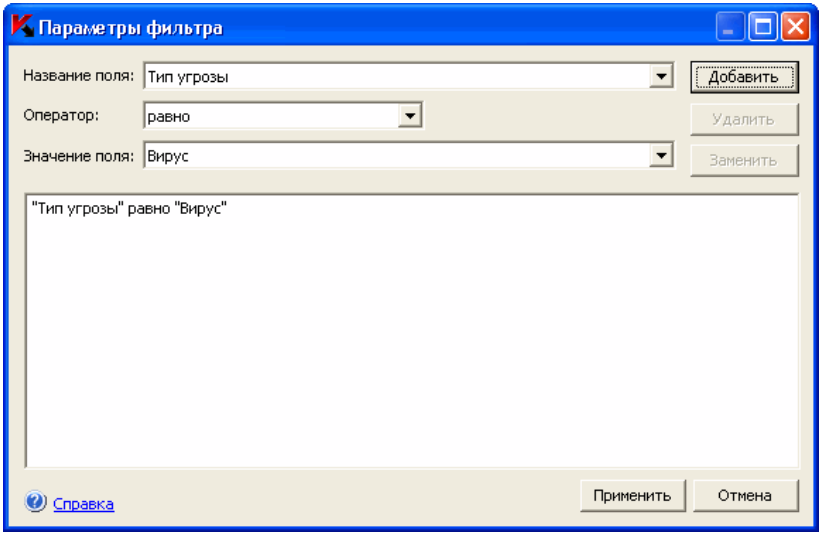

Рисунок 81. Диалоговое окно **Параметры фильтра**

2. Чтобы добавить фильтр:

   а) В списке **Название поля** выберите поле, с которым будет сравниваться значение фильтра.

   б) В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в поле **Название поля**.

   в) В поле **Значение поля** введите или выберите значение фильтра из списка возможных.

   г) Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого фильтра, который вы хотите добавить.

- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
- Чтобы отредактировать фильтр, выберите фильтр в списке в диалоговом окне **Параметры фильтра**, затем измените нужные значения в полях **Название поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить**.

3. После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке объектов в подробном отчете отобразятся только объекты, отобранные согласно заданным вами фильтрам.

*Чтобы снова отобразить все объекты, нажмите на кнопку **Снять фильтр** в нижней части диалогового окна **Подробный отчет**.*

13.2.5. Экспорт информации из подробного отчета в текстовый файл

Чтобы экспортировать информацию из подробного отчета в текстовый файл:

1. В дереве консоли выберите узел **Отчеты**.
2. В списке отчетов откройте контекстное меню на сводном отчете о задаче, подробный отчет о событиях в которой вы хотите просмотреть, выберите команду **Просмотреть отчет**.
3. В нижней части диалогового окна **Подробный отчет** нажмите на кнопку **Экспорт** и в диалоговом окне **Обзор** задайте имя для файла, в котором вы хотите сохранить информацию из подробного отчета и кодировку (Юникод или ANSI).

13.2.6. Удаление отчетов

По умолчанию отчеты хранятся ограниченное время (вы можете изменять срок хранения отчетов с помощью общего параметра Антивируса **Срок хранения отчетов**, см. п. 3.2 на стр. 46).

В узле **Отчеты** вы можете удалять выбранные отчеты о завершившихся задачах.

Чтобы удалить один или несколько отчетов:

1. В дереве консоли выберите узел **Отчеты**.
2. Выполните одно из следующих действий:
   - чтобы удалить один отчет, в списке отчетов откройте контекстное меню на отчете, который вы хотите удалить, и выберите команду **Удалить**;
   - чтобы удалить несколько отчетов, выберите нужные отчеты в списке, используя клавишу **<Ctrl>** или клавишу **<Shift>**, затем

откройте контекстное меню на любом из выбранных отчетов и выберите команду **Удалить**.

В диалоговом окне **Подтверждение** выберите **Да**, чтобы подтвердить операцию. Выбранные отчеты будут удалены.

13.2.7. Настройка уровня детализации информации в отчетах и журнале событий

С помощью описанных ниже параметров вы можете указать, какие события будут регистрироваться в подробных отчетах о выполнении задач отдельных функциональных компонентов Антивируса и какие события будут регистрироваться в журнале событий. О журнале событий Антивируса читайте в п. 13.5 на стр. 226.

По уровню важности события Антивируса, связанные с выполнением задач, делятся на три типа: *информационные*, *важные* и *критические*:

Информационные события, например *Угроз не обнаружено* или *Нет ошибок*, отражают результаты работы Антивируса.

Важные события, такие как *Ошибка соединения с источником обновления*, могут повлиять на выполнение функций Антивируса.

Критические события могут привести к нарушению антивирусной безопасности защищаемого сервера. К ним относятся, например, события *Целостность модуля нарушена*, *Обнаружена угроза* или *Внутренняя ошибка задачи*.

Уровень детализации в подробных отчетах о выполнении задач и журнале событий соответствует уровню важности событий, которые в нем регистрируются. Вы можете установить один из трех уровней детализации от **Информационного**, при котором регистрируются события всех уровней важности, до **Критического**, при котором регистрируются только критические события. По умолчанию для всех компонентов кроме компонента **Обновление** установлен уровень детализации **Важные события** (регистрируются только важные и критические события); для компонента **Обновление** установлен уровень **Информационные события**.

Вы также можете вручную указать отдельные события для регистрации в подробных отчетах и журнале событий.

Чтобы задать уровень детализации событий в подробных отчетах о выполнении задач и журнале событий:

1. В дереве консоли откройте контекстное меню на узле **Отчеты** и выберите команду **Свойства**.
2. В диалоговом окне **Свойства: Отчеты** (см. рис. 82) в списке **Компонент** выберите функциональный компонент Антивируса, для задач которого вы хотите задать уровень детализации событий.

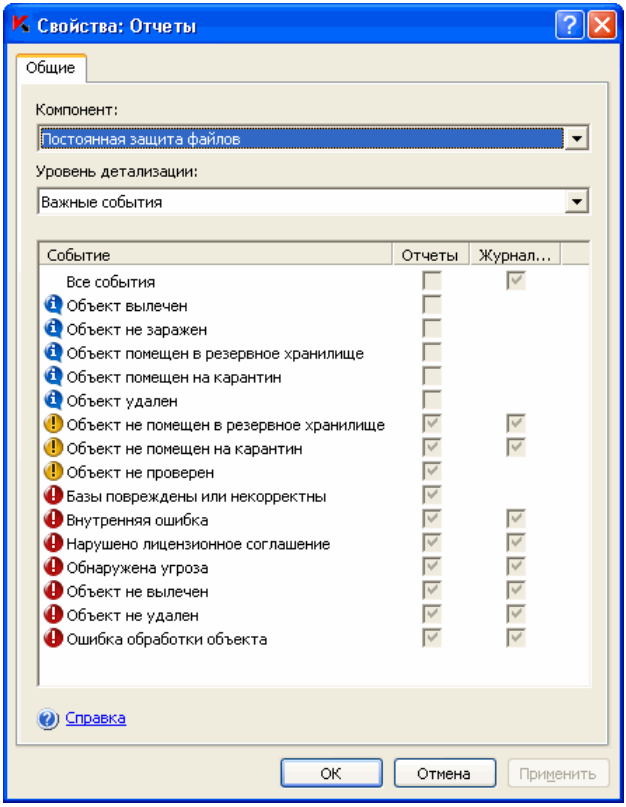

Рисунок 82. Диалоговое окно **Свойства: Отчеты**

3. Выполните одно из следующих действий:
   - чтобы задать уровень детализации в подробных отчетах о выполнении задач выбранного функционального компонента, выберите нужный уровень в списке **Уровень детализации**.

В списке событий будут установлены флажки рядом с событиями, которые будут включены в отчеты и журнал событий в соответствии с выбранным уровнем детализации.

- чтобы включить регистрацию отдельных событий функционального компонента, в списке **Уровень детализации** выберите **Другой**, а затем в списке событий компонента выполните следующие действия:
  - чтобы включить регистрацию события в подробных отчетах о выполнении задач, установите соответствующий событию флажок **Отчеты**; чтобы отключить регистрацию события в подробных отчетах, снимите соответствующий событию флажок **Отчеты**.
  - чтобы включить регистрацию события в журнале событий, установите соответствующий событию флажок **Журнал событий**; чтобы отключить регистрацию события в журнале событий, снимите соответствующий событию флажок **Журнал событий**.

4. Нажмите на кнопку **ОК**.

13.3. Журнал системного аудита

Антивирус ведет системный аудит событий, связанных с управлением Антивирусом, таких как запуск Антивируса, запуск и остановка задач, изменение параметров задач, создание и удаление задач проверки по требованию и других. Записи об этих событиях отображаются в узле **Журнал системного аудита**.

По умолчанию Антивирус хранит записи в журнале системного аудита неограниченное время. Вы можете ограничить длительность хранения записей с помощью общего параметра Антивируса **Срок хранения событий в журнале** системного аудита (см. п. 3.2 на стр. 46).

*Чтобы просмотреть события в журнале системного аудита, в дереве консоли выберите узел **Журнал системного аудита** (см. рис. 83).*

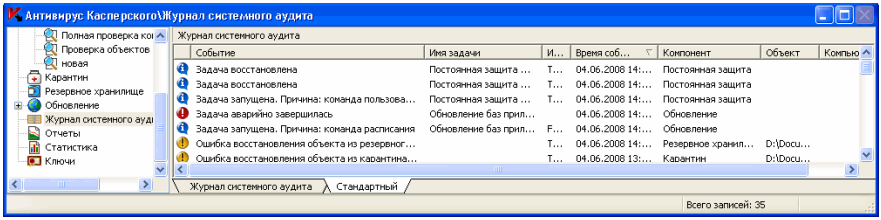

Рисунок 83. Узел **Журнал системного аудита**

В панели результатов отображается следующая информация о событиях:

Поле	Описание
Событие	Описание события; включает тип события и дополнительную информацию о нем. По уровню важности события делятся на *информационные*, *важные* и *критические*.
Имя задачи	Имя задачи Антивируса, с выполнением которой связано событие.
Имя пользователя	Если событие вызвал пользователь Антивируса, то в этом столбце отображается имя пользователя. Если действие вызвал не пользователь, а сам Антивирус, например, запустил по расписанию задачу проверки по требованию, этот столбец содержит запись **<домен><имя компьютера>$**, что соответствует учетной записи **Локальная система**.
Время события	Время регистрации события по часам защищаемого сервера в формате, установленном региональными настройками Microsoft Windows сервера.
Компонент	Функциональный компонент Антивируса, в работе которого возникло событие. Если событие связано не с работой отдельных компонентов, а с работой Антивируса в целом, например, запуск Антивируса, в этом столбце содержится запись **Приложение**.
Объект	Имя объекта, с обработкой которого связано событие (только для компонентов **Карантин** и **Резервное хранилище**).

Компьютер	Имя компьютера, доступ с которого к серверу был заблокирован или разрешен (только для функции **Блокирование доступа с компьютеров**).

Вы можете выполнять следующие действия над событиями в узле **Системый аудит**:

- сортировать события (см. п. 13.3.1 на стр. 219);
- фильтровать события (см. п. 13.3.2 на стр. 219);
- удалять события (см. п. 13.3.3 на стр. 221).

13.3.1. Сортировка событий в журнале системного аудита

По умолчанию события отображаются в узле **Журнал системного аудита** в обратном хронологическом порядке.

Чтобы найти событие в списке, вы можете отсортировать события по содержимому любого из столбцов с информацией. Результат сортировки сохранится, если вы покинете и снова выберете узел **Журнал системного аудита** или если вы закроете консоль Антивируса с сохранением в *msc*-файл и снова откроете ее из этого файла.

Чтобы отсортировать события:

1. В дереве консоли выберите узел **Журнал системного аудита**.
2. В панели результатов щелкните на заголовке столбца, по содержимому которого вы хотите отсортировать события в списке.

13.3.2. Фильтрация событий в журнале системного аудита

Чтобы найти событие в журнале системного аудита, вы можете *отфильтровать события* – отобразить в списке только те события, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

Результат фильтрации сохранится, если вы покинете и снова выберете узел **Журнал системного аудита** или если вы закроете консоль Антивируса с сохранением в *msc*-файл и снова откроете ее из этого файла.

Чтобы отфильтровать события в журнале системного аудита:

1. В дереве консоли откройте контекстное меню на узле **Журнал системного аудита** и выберите команду **Фильтр**.

   Откроется диалоговое окно **Параметры фильтра** (см. рис. 84).

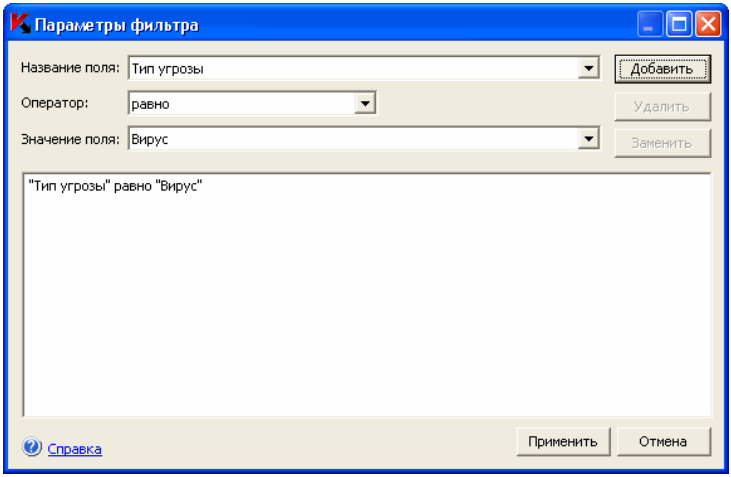

Рисунок 84. Диалоговое окно **Параметры фильтра**

2. Чтобы добавить фильтр:

   а) В списке **Название поля** выберите поле, с которым будет сравниваться значение фильтра.

   б) В списке **Оператор** выберите условие фильтрации. Условия фильтрации могут быть различными в зависимости от того, какое значение вы выберите в поле **Название поля**.

   в) В поле **Значение поля** введите или выберите значение фильтра из списка возможных.

   г) Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого фильтра, который вы хотите добавить. Если вы зададите несколько фильтров, то они объединятся по логическому «И».

- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
- Чтобы отредактировать фильтр, выберите его в списке фильтров в диалоговом окне **Параметры фильтра**, затем измените нужные

значения в полях **Название поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить**.

3. После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке событий отобразятся только события, отобранные согласно заданным вами фильтрам.

*Чтобы снова отобразить все события, в дереве консоли откройте контекстное меню на узле **Журнал системного аудита** и выберите команду **Снять фильтр**.*

13.3.3. Удаление событий из журнала системного аудита

По умолчанию Антивирус хранит события в журнале системного аудита неограниченное время. Вы можете ограничить срок хранения событий (см. настройку параметра **Срок хранения событий в журнале системного аудита** в п. 3.2 на стр. 46).

Вы можете вручную удалить все события из журнала системного аудита.

Чтобы удалить все события из журнала системного аудита:

1. В дереве консоли откройте контекстное меню на узле **Журнал системного аудита** и выберите команду **Очистить**.
2. В диалоговом окне **Подтверждение** выберите **Да**, чтобы подтвердить операцию.

13.4. Статистика Антивируса

Статистика Антивируса – это информация о текущем состоянии Антивируса, состоянии его функциональных компонентов и выполняемых задач.

*Чтобы просмотреть статистику Антивируса, в дереве консоли выберите узел **Статистика**.*

В панели результатов отображается следующая информация об Антивирусе:

- ссылка на страницу Антивируса в интернете;
- версия Антивируса и дата его установки;
- информация об активном ключе: серийный номер, тип, дата окончания срока действия и информация о скором окончании:

– до окончания срока действия ключа не менее 14 дней;

– до окончания срока действия ключа менее 14, но не менее 7 дней;

– до окончания срока действия ключа осталось менее 7 дней.

Вы можете настроить уведомление администратора о скором окончании срока действия ключа (см. п. 15.2 на стр. 237).

- состояние и параметры функциональных компонентов Антивируса; состояние и статистика выполняемых задач (см. описание в таблице 15).

По умолчанию информация в узле **Статистика** обновляется ежеминутно. Вы можете обновлять информацию в узле **Статистика** по требованию.

*Чтобы вручную обновить информацию в узле **Статистика**, откройте контекстное меню на узле **Статистика** и выберите команду **Обновить**.*

Таблица 15. Информация о функциональных компонентах Антивируса и выполняемых задачах в узле **Статистика**

Компонент / Задача	**Информация в узле Статистика**
Задача **Постоянная защита файлов**	Состояние задачи: ВЫПОЛНЯЕТСЯ – задача выполняется; ОСТАНОВЛЕНА – задача приостановлена или остановлена. Статистика задачи: **Обнаружено угроз** – количество угроз, обнаруженных с момента запуска задачи; **Предотвращение вирусных эпидемий**: • **Активировано** – Антивирус повысил уровень защиты в задаче **Постоянная защита файлов** в соответствии с параметрами «Предотвращение вирусных эпидемий» (подробнее читайте в п. A.4.4 на стр. 422); • **Не активировано** – в текущий момент Антивирус не применяет режим «Предотвращение вирусных эпидемий»; **Проверено объектов** – количество проверенных объектов с момента последнего запуска задачи.

Компонент / Задача	**Информация в узле Статистика**
	Если задача **Постоянная защита файлов** выполняется, то ссылка **Подробнее** открывает диалоговое окно **Статистика выполнения задачи** (см. п. 6.3 на стр. 90).
Блокирование доступа с компьютеров	Состояние автоматического блокирования доступа с компьютеров:  – выполняется задача **Постоянная защита файлов** и включено автоматическое блокирование доступа с компьютеров; ссылка **Подробнее** открывает диалоговое окно **Статистика** (см. п. 7.9 на стр. 106);  – выключено. Статистика блокирования: **Компьютеров в списке блокирования** – количество компьютеров в списке блокирования в текущий момент
Задача **Проверка скриптов**	Состояние задачи:  ВЫПОЛНЯЕТСЯ – задача выполняется;  ОСТАНОВЛЕНА – задача приостановлена или остановлена. Статистика задачи: **Обнаружено угроз** – количество угроз, обнаруженных с момента запуска задачи; **Обработано объектов** – количество скриптов, обработанных с момента последнего запуска задачи; **Заблокировано скриптов** – количество подозрительных или опасных скриптов, которые Антивирус обнаружил с момента запуска задачи и заблокировал; Если задача запущена, то ссылка **Подробнее** открывает диалоговое окно **Статистика выполнения задачи** (см. п. 6.5 на стр. 94).

Компонент / Задача	Информация в узле Статистика
Актуальность баз	Общее состояние баз Антивируса на защищаемом сервере:  – базы актуальны;  – базы устарели;  – базы сильно устарели. Подробнее об актуальности баз читайте в п. 10.1 на стр. 149. **Дата создания баз** – дата и время создания последних установленных обновлений баз; **Количество записей в базах** – общее количество записей в базах, используемых в текущий момент.
Карантин	Общее состояние карантина (отображается, если применяются параметры **Максимальный размер карантина** и **Порог свободного пространства в карантине**):  – максимальный размер карантина не достигнут; порог свободного пространства в карантине не достигнут;  – максимальный размер карантина не достигнут, но достигнут порог свободного пространства в карантине;  – достигнут максимальный размер карантина. Когда объем данных в папке каратнина достигает значений указанных параметров, Антивирус уведомляет об этом администратора (если настроены уведомления об этих событиях). Антивирус продолжает помещать объекты на карантин. Информацию о том, как настроить уведомления, содержит Глава 15 на стр. 234. О том, как настроить параметры карантина, см. п. 11.8 на стр. 185. Статистика карантина: **Объектов на карантине** – количество объектов на карантине в текущий момент; **Занятое пространство** – объем данных в папке карантина. Ссылка **Подробнее** открывает диалоговое окно **Статистика карантина** (см. п. 11.9 на стр. 187).

Компонент / Задача	**Информация в узле Статистика**
Резервное хранилище	Общее состояние резервного хранилища (отображается, если применяются параметры **Максимальный размер резервного хранилища** и **Порог свободного пространства в хранилище**):  – максимальный размер резервного хранилища не достигнут; порог свободного пространства в резервном хранилище не достигнут;  – максимальный размер резервного хранилища не достигнут, но достигнут порог свободного пространства в нем;  – достигнут максимальный размер резервного хранилища. Когда объем данных в резервном хранилище достигает значений указанных параметров, Антивирус уведомляет об этом администратора (если настроены уведомления об этих событиях). Антивирус продолжает помещать файлы в резервное хранилище. Информацию о том, как настроить уведомления, содержит Глава 15 на стр. 234. О том, как настроить параметры резервного хранилища, см. п. 12.5 на стр. 199. Статистика резервного хранилища: **Объектов в резервном хранилище** – количество файлов в резервном хранилище в текущий момент; **Занятое пространство** – объем занятого пространства в резервном хранилище. Ссылка **Подробнее** открывает диалоговое окно **Статистика резервного хранилища** (см. п. 12.6 на стр. 201).

13.5. Журнал событий Антивируса в консоли «Просмотр событий»

С помощью консоли MMC Microsoft Windows «Просмотр событий» (Event Viewer) вы можете просматривать журнал событий Антивируса. В нем Антивирус регистрирует события, важные с точки зрения антивирусной безопасности защищаемого сервера и диагностики сбоев Антивируса.

Вы можете выбирать события для регистрации в журнале событий:

- по типам событий;
- по уровню детализации. Уровень детализации соответствует уровню важности событий, которые в нем регистрируются (*информационные*, *важные* или *критические события*). Наиболее подробным является *информационный*, при котором регистрируются события всех уровней важности; наименее подробным является *критический*, при котором регистрируются только критические события. По умолчанию для всех компонентов кроме компонента **Обновление** установлен уровень детализации **Важные события** (регистрируются только важные и критические события); для компонента **Обновление** установлен уровень **Информационные события**.

О том, как выбрать события для регистрации в журнале событий, см. п. 13.2.7 на стр. 215.

Чтобы просмотреть журнал событий:

1. Добавьте в консоль MMC оснастку «Просмотр событий». Если вы управляете защитой сервера удаленно, с рабочего места администратора, укажите защищаемый сервер в качестве компьютера, которым оснастка должна управлять.
2. В дереве консоли «Просмотр событий» выберите узел **Антивирус Касперского** (см. рис. 85).

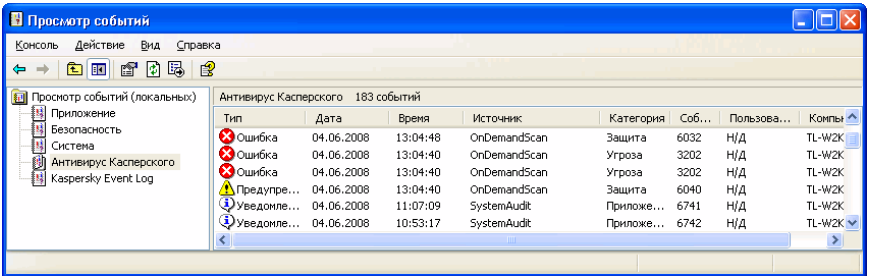

Рисунок 85. Информация о событиях Антивируса в консоли «Просмотр событий»

ГЛАВА 14. УСТАНОВКА И УДАЛЕНИЕ КЛЮЧЕЙ

В этой главе содержится следующая информация:

14.1. О ключах Антивируса

Ключ представляет собой текстовый файл с расширением .key. Он содержит информацию о правах на использование Антивируса и ограничениях.

При выписке ключа устанавливается предельная дата – *дата, после которой ключ становится недействительным* (например, 31 декабря 2010, если ключ выписан в 2007 году), а также устанавливается *период действия ключа* в днях (например, 365 дней). «Лаборатория Касперского» может выписывать ключи с различными периодами действия.

При установке ключа Антивирус рассчитывает *дату окончания срока действия ключа* – эта дата наступает по истечении периода действия ключа с момента его установки, но не позднее даты, после которой ключ становится недействительным. В течение этого времени вам доступны следующие возможности:

- антивирусная защита;
- поддержка баз в актуальном состоянии (обновление баз);
- получение срочных обновлений модулей Антивируса (patch);
- возможность установки плановых обновлений Антивируса (upgrade).

В течение этого периода «Лаборатория Касперского» или ее партнер оказывает вам техническую поддержку, если это предусмотрено условиями предоставления ключа.

После *даты окончания срока действия ключа* Антивирус прекращает выполнять свои функции: в зависимости от типа ключа вы не сможете пользоваться или только функциями обновления баз и модулей Антивируса и технической поддержкой или всеми функциям Антивируса.

В Антивирусе предусмотрены три типа ключей: *для бета-тестирования*, *пробный* и *коммерческий.*

Ключ для бета-тестирования

Ключ для бета-тестирования предоставляется бесплатно. Он выписывается только в период бета-тестирования Антивируса. После завершения срока действия ключа Антивирус прекращает выполнять все свои функции.

Пробный ключ

Пробный ключ также предоставляется бесплатно. Он предназначен для ознакомления с Антивирусом. Пробный ключ имеет небольшой период действия; после завершения срока действия ключа Антивирус прекращает выполнять все свои функции. Вы можете установить только один пробный ключ Антивируса.

Коммерческий ключ

После окончания срока действия коммерческого ключа Антивирус продолжает выполнять все свои функции кроме функций обновления. Он проверяет сервер, используя базы, установленные до даты окончания срока действия ключа. Он не выявляет угрозы, информацию о которых специалисты «Лаборатории Касперского» занесли в базы после окончания срока действия ключа и не лечит объекты, зараженные этими угрозами. Техническая поддержка также предоставляется только на период действия ключа.

Вы можете приобрести и установить сразу два ключа: один – в качестве активного, другой – в качестве резервного. *Активный* ключ начинает действовать с момента его установки, а *резервный* ключ вступает в действие автоматически, когда завершается срок действия активного ключа.

Ключ Антивируса может иметь ограничение на использование по количеству серверов.

14.2. Просмотр информации об установленных ключах

Чтобы просмотреть информацию об установленных ключах:

1. В дереве консоли выберите узел **Ключи**.
2. В панели результатов откройте контекстное меню на строке с информацией о ключе, сведения о котором вы хотите просмотреть, и выберите команду **Свойства**.

   Откроется диалоговое окно **Свойства: <Серийный номер ключа>** (см. рис. 86).

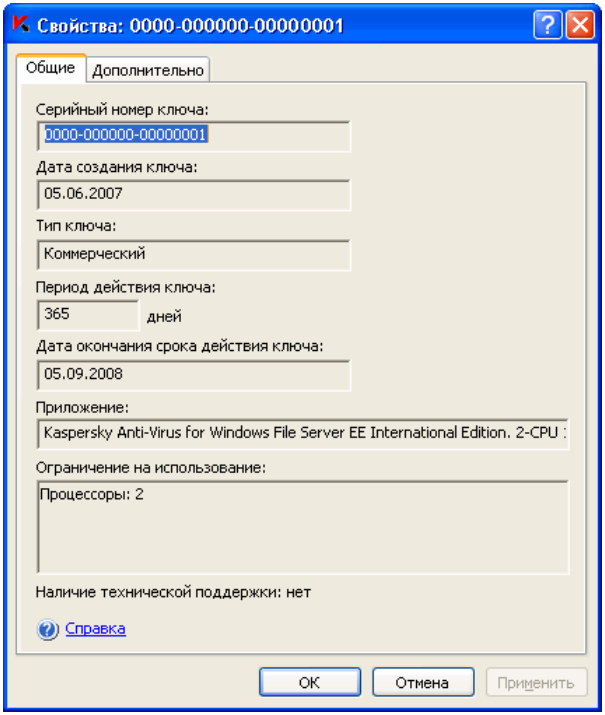

Рисунок 86. Диалоговое окно **Свойства ключа**, закладка **Общие**

В диалоговом окне **Свойства: <Серийный номер ключа>** на закладке **Общая** отображается следующая информация:

Таблица 16. Информация об установленном ключе

Поле	Описание
Серийный номер ключа	Серийный номер ключа.
Дата создания ключа	Дата выписки ключа.
Тип ключа	Тип ключа (для бета-тестирования, пробный или коммерческий). Подробнее о типах ключей читайте в п. 14.1 на стр. 228.
Период действия ключа	Период действия ключа в днях, устанавливается при его выписке.
Дата окончания срока действия ключа	Дата окончания срока действия ключа; рассчитывается Антивирусом при установке ключа; наступает, когда завершается *период действия* ключа с момента его активации, но не позднее *даты, когда ключ становится недействительным*.
Приложение	Название Антивируса.
Ограничение на использование	Предусмотренное ключом ограничение (если имеется).
Наличие технической поддержки	Информация о том, оказывает ли «Лаборатория Касперского» или ее партнер техническую поддержку заказчику по условиям предоставления ключа.

В диалоговом окне **Свойства: <Серийный номер ключа>** на закладке **Дополнительно** отображается информация о заказчике, а также контактная информация «Лаборатории Касперского» или партнера, у которого вы приобрели Антивирус.

14.3. Установка ключа

Чтобы установить ключ:

1. В дереве консоли откройте контекстное меню на узле **Ключи** и выберите команду **Установить ключ**.
2. В диалоговом окне **Добавление ключа** (см. рис. 87) укажите имя файла ключа и путь к файлу.

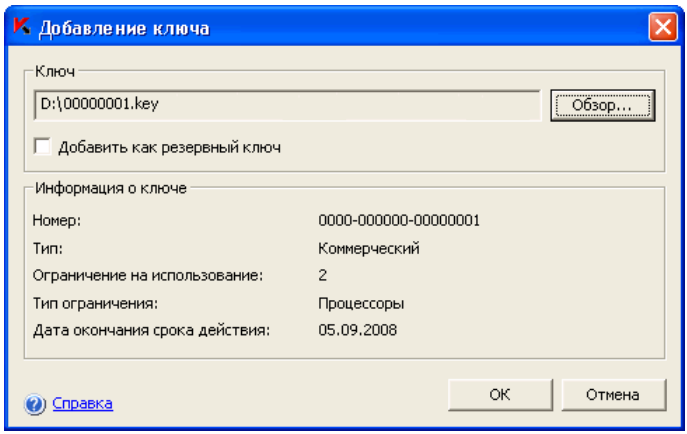

Рисунок 87. Диалоговое окно **Добавление ключа**

В диалоговом окне отобразится информация о ключе, описанная в таблице ниже.

3. Если вы устанавливаете ключ в качестве резервного, то установите флажок **Добавить как резервный ключ**.
4. Нажмите на кнопку **ОК**.

В диалоговом окне **Добавление ключа** отображается следующая информация об устанавливаемом ключе:

Таблица 17. Информация о ключе

Поле	Описание
Номер	Серийный номер ключа
Тип	Тип ключа (для бета-тестирования, пробный или коммерческий). Подробнее о типах ключей читайте в п. 14.1 на стр. 228.

Ограничение на использование	Количество объектов ограничения
Тип ограничения	Объекты ограничения
Дата окончания срока действия	Дата окончания срока действия ключа; рассчитывается Антивирусом; наступает, когда завершается *период действия* ключа с момента его активации, но не позднее *даты, когда ключ становится недействительным*. Подробнее см. в п. 14.1 на стр. 228.

14.4. Удаление ключа

Вы можете удалить установленный ключ.

Если вы удалите активный ключ при установленном резервном, резервный ключ автоматически станет активным.

Внимание!

Если вы удалите установленный ключ, вы сможете восстановить его, только установив повторно из файла ключа.

Чтобы удалить установленный ключ:

1. В дереве консоли выберите узел **Ключи**.
2. В панели результатов откройте контекстное меню на строке с информацией о ключе, который вы хотите удалить, и выберите команду **Удалить ключ**.
3. В диалоговом окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить удаление ключа.

ГЛАВА 15. НАСТРОЙКА УВЕДОМЛЕНИЙ

В этой главе содержится следующая информация:

- способы уведомления администратора и пользователей (см. п. 15.1 на стр. 234);
- настройка уведомлений (см. п. 15.2 на стр. 237).

15.1. Способы уведомления администратора и пользователей

Антивирус позволяет уведомлять администратора и пользователей, которые обращаются к защищаемому серверу, о событиях, связанных с работой Антивируса и состоянием антивирусной защиты сервера:

- администратор может получать информацию о событиях выбранных типов;
- пользователи локальной сети, которые обращаются к защищаемому серверу, могут получать информацию о событиях типов *Обнаружена угроза* и *Компьютер добавлен в список блокирования*; терминальные пользователи сервера могут получать информацию о событиях *Обнаружена угроза*.

В консоли ММС Антивируса вы можете настроить уведомления администратора или пользователей несколькими способами. Эти способы описаны в следующих таблицах.

Таблица 18. Способы уведомлений пользователей

Способ уведомления	**Настройка по умолчанию**	**Описание**
Окна службы терминалов	Настроен по событиям *Обнаружена угроза*	Если защищаемый сервер является терминальным, вы можете применять этот способ для оповещения терминальных пользователей сервера.
Окна Службы сообщений Microsoft Windows	Настроен по событиям *Обнаружена угроза* и *Компьютер добавлен в список блокирования*	Этот способ уведомления использует Службу сообщений Microsoft Windows. Перед тем как использовать этот способ уведомлений, убедитесь, что Служба сообщений включена на защищаемом сервере и рабочих станциях пользователей локальной сети (по умолчанию она выключена).

Таблица 19. Способы уведомлений администраторов

Способ уведомления	**Настройка по умолчанию**	**Описание**
Уведомление средствами Службы сообщений Microsoft Windows	Не настроен	Этот способ уведомлений использует Службу сообщений Microsoft Windows. Перед тем как настроить этот способ уведомления, убедитесь, что Служба сообщений включена на защищаемом сервере и компьютере, который играет роль рабочего места администратора (если администратор управляет Антивирусом удаленно). По умолчанию Служба сообщений выключена.
Запуск исполняемого файла	Не настроен	Этот способ уведомления запускает по событию указанный исполняемый файл. Исполняемый файл должен храниться на локальном диске защищаемого сервера.

Способ уведомления	Настройка по умолчанию	Описание
Уведомление по электронной почте	Не настроен	Этот способ уведомления использует для передачи уведомлений электронную почту.

Вы можете создавать текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии.

Текст сообщений, который используется по умолчанию для уведомлений пользователей, приводится в следующей таблице.

Таблица 20. Текст сообщений для уведомления пользователей, составленный по умолчанию

Задача	Тип события	Текст сообщения
Постоянная защита файлов	*Обнаружена угроза*	Антивирус Касперского заблокировал доступ к %OBJECT% на компьютере %FROM_COMPUTER% в %EVENT_TIME% Причина: %EVENT_TYPE%. Тип угрозы: %VIRUS_TYPE%: %VIRUS_NAME%. Имя пользователя объекта: %USER_NAME%. Имя компьютера пользователя объекта: %USER_COMPUTER%
Постоянная защита файлов, функция *Блокирование доступа с компьютеров*	*Компьютер добавлен в список блокирования*	Антивирус Касперского на компьютере %FROM_COMPUTER%: %EVENT_TYPE%. Имя компьютера: %USER_COMPUTER%. Время блокирования: %EVENT_TIME%. Обратитесь к системному администратору вашей сети

15.2. Настройка уведомлений

Настройка уведомлений о событии предполагает выбор и настройку способа уведомлений и составление текста сообщения.

Чтобы настроить уведомления о событиях:

1. В дереве консоли откройте контекстное меню на названии оснастки Антивируса и выберите команду **Настроить уведомления**.

   Откроется диалоговое окно **Уведомления** (см. рис. 88).

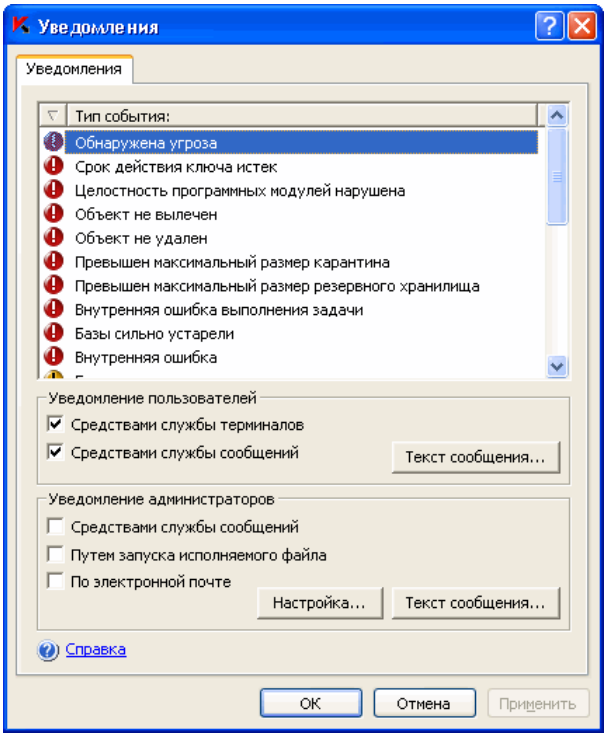

Рисунок 88. Диалоговое окно **Уведомления**

2. В диалоговом окне **Уведомления** на закладке **Уведомления** выберите события и укажите способ уведомлений для них:

   - чтобы указать способы уведомлений администратора, выполните следующие действия:

     а) в списке **Тип события** выберите событие, для которого вы хотите выбрать способ уведомления;

     б) в группе параметров **Уведомление администраторов** установите флажок рядом со способами уведомлений, которые вы хотите настроить;

   - чтобы указать способы уведомлений пользователей, выполните следующие действия:

     а) в списке **Тип события** выберите типы событий, о которых Антивирус будет уведомлять пользователей (вы можете выбрать события *Обнаружена угроза* и *Компьютер добавлен в список блокирования*);

     б) в группе параметров **Уведомление пользователей** установите флажок рядом со способами уведомлений, которые вы хотите настроить.

     Примечание

     Вы можете составить один текст сообщения для нескольких типов событий: после того как вы выбрали способ уведомлений для одного типа событий, выберите, используя клавишу **<Ctrl>** или клавишу **<Shift>**, остальные типы событий, для которых вы хотите составить такой же текст сообщения.

3. Чтобы составить текст сообщения, нажмите на кнопку **Текст сообщения** в нужной группе параметров и в диалоговом окне **Текст сообщения** введите текст, который будет отображаться в сообщении о событии.

   Чтобы добавить поля с информацией о событии, нажмите на кнопку **Макрос** и выберите нужные поля из списка возможных. Поля с информацией о событиях описаны в таблице 21.

   Чтобы вернуть текст сообщения, по умолчанию предусмотренный для события, нажмите на кнопку **По умолчанию**.

4. Чтобы настроить выбранные способы уведомлений администраторов о выбранных событиях, в диалоговом окне **Уведомления** нажмите на кнопку **Настройка** и в диалоговом окне **Дополнительная настройка** выполните настройку выбранных способов.

- Для уведомлений по электронной почте откройте закладку **Электронная почта** (см. рис. 89) и в соответствующих полях укажите электронные адреса получателей (разделяйте адреса символом «точка с запятой»), имя или сетевой адрес SMTP-сервера, а также его порт. Если требуется, укажите текст, который будет отображаться в полях **Тема** и **От**. В текст поля **Тема** вы также можете включать значения полей с информацией о событии (см. таблицу 21).

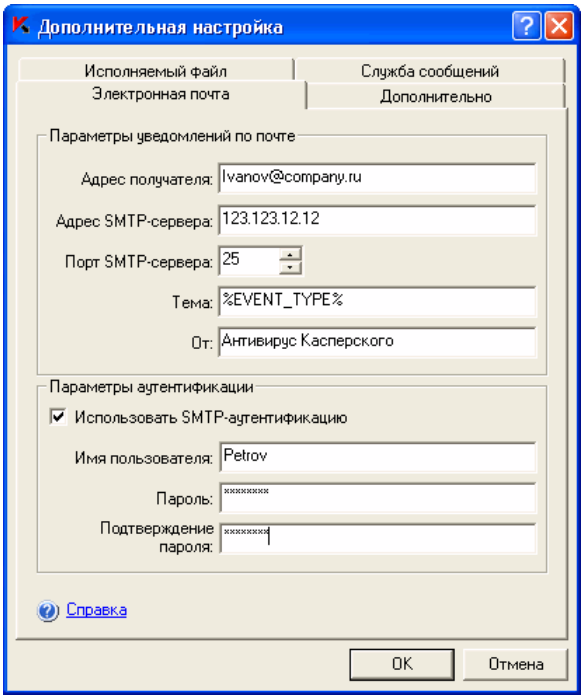

Рисунок 89. Диалоговое окно **Дополнительная настройка**, закладка **Электронная почта**

Если вы хотите использовать проверку подлинности по учетной записи при соединении с SMTP-сервером, то в группе **Параметры аутентификации** установите флажок **Использовать SMTP-аутентификацию** и укажите имя и пароль пользователя, учетная запись которого будет проверяться.

- Для уведомлений через службу сообщений на закладке **Служба сообщений** (см. рис. 90), составьте список компьютеров-получателей уведомлений: для каждого компьютера, который

вы хотите добавить, нажмите на кнопку **Добавить** и в поле ввода введите его сетевое имя. Не указывайте в этом поле IP-адреса компьютеров.

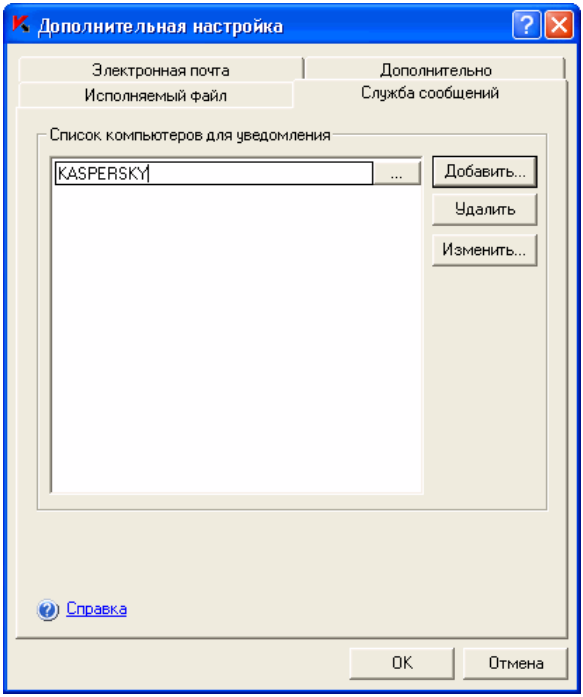

Рисунок 90. Диалоговое окно **Дополнительная настройка**, закладка **Служба сообщений**

- Для запуска исполняемого файла на закладке **Исполняемый файл** (см. рис. 91) выберите на локальном диске защищаемого сервера файл, который будет выполняться на сервере по событию, или введите полный путь к нему. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

  Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

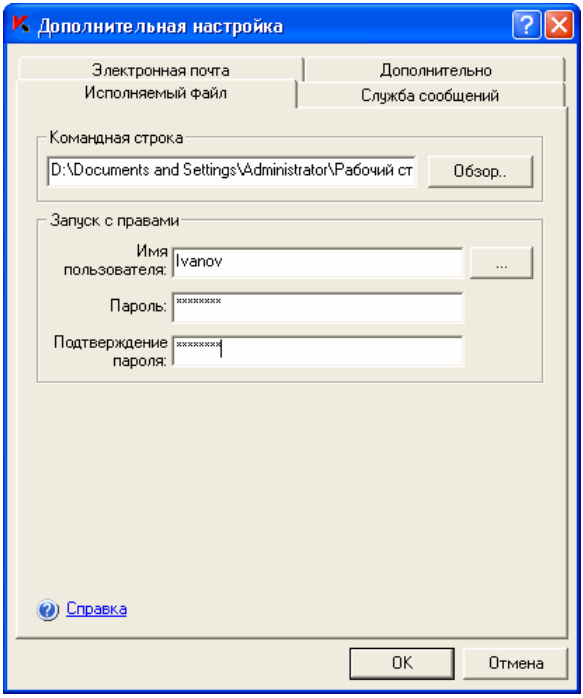

Рисунок 91. Диалоговое окно **Дополнительная настройка**, закладка **Исполняемый файл**

- Если вы хотите ограничить количество уведомлений по событиям одного типа в единицу времени, на закладке **Дополнительно** (см. рис. 92) установите флажок **Не отправлять одно и то же уведомление чаще** и укажите нужное количество раз и единицу времени.

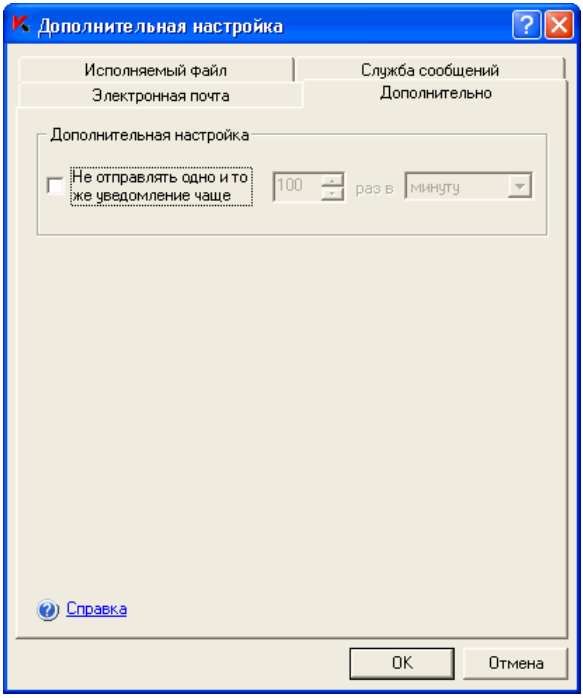

Рисунок 92. Диалоговое окно **Дополнительная настройка**, закладка **Дополнительно**

5. Нажмите на кнопку **ОК**.

Таблица 21. Поля с информацией о событии

Поле	Описание
%EVENT_TYPE%	Тип события.
%EVENT_TIME%	Время возникновения события.
%EVENT_SEVERITY%	Уровень важности события.
%OBJECT%	Имя объекта (в задачах постоянной защиты и проверки по требованию). В задаче **Обновление модулей приложения** включает название обновления и адрес страницы в интернете с информацией об обновлении.

Поле	Описание
%VIRUS_NAME%	Имя угрозы по классификации «Лаборатории Касперского»; входит в полное название угрозы, которое возвращает Антивирус (в задачах постоянной защиты и проверки по требованию).
%VIRUS_TYPE%	Тип угрозы по классификации «Лаборатории Касперского»; входит в полное название угрозы, которое возвращает Антивирус (в задачах постоянной защиты и проверки по требованию).
%USER_COMPUTER%	В задаче **Постоянная защита файлов** имя компьютера пользователя, который обратился к объекту на сервере.
%USER_NAME%	В задаче **Постоянная защита файлов** имя пользователя, который обратился к объекту на сервере.
%FROM_COMPUTER%	Имя защищаемого сервера, с которого поступило уведомление.
%REASON%	Причина возникновения события (некоторые события не имеют этого поля).
%ERROR_CODE%	Код ошибки (применяется только для события *внутренняя ошибка задачи*).
%TASK_NAME%	Имя задачи (имеется только у событий, связанных с выполнением задач).

ЧАСТЬ 2. УПРАВЛЕНИЕ АНТИВИРУСОМ ИЗ КОМАНДНОЙ СТРОКИ

В этой части содержится следующая информация:

- описание команд управления Антивирусом из командной строки (Глава 16 на стр. 245);
- описание кодов возврата (Глава 17 на стр. 267).

ГЛАВА 16. КОМАНДЫ УПРАВЛЕНИЯ АНТИВИРУСОМ ИЗ КОМАНДНОЙ СТРОКИ

Вы можете выполнять основные команды управления Антивирусом из командной строки защищаемого сервера, если при установке Антивируса вы включили в список устанавливаемых компонентов компонент **Утилита командной строки**.

С помощью команд командной строки вы можете управлять только функциями, доступными вам в соответствии с вашими правами в Антивирусе (подробнее правах доступа к функциям Антивируса читайте в п. 2.6.1 на стр. 40).

Некоторые из команд Антивируса выполняются в синхронном режиме: управление возвращается на консоль только после завершения выполнения команды; другие команды выполняются в асинхронном режиме: управление возвращается на консоль сразу после запуска команды.

Чтобы прервать выполнение команды в синхронном режиме, нажмите <**Ctrl+C**>.

При вводе команд Антивируса применяйте следующие правила:

- вводите ключи и команды символами верхнего или нижнего регистра;
- разделяйте ключи символом пробела;
- если имя файла, которое вы указываете в качестве значения ключа, содержит символ пробела, заключите это имя файла (и путь к нему) в кавычки, например: “C:\TEST\test cpp.exe”;
- в масках имен файлов или путей используйте только один заместительный символ и вводите его только в конце пути к папке или файлу, например: "C:\Temp\Temp*\", "C:\Temp\Temp???.doc", "C:\Temp\Temp*.doc"

Список команд Антивируса приводится в таблице 22.

Глава 17 на стр. 267 содержит коды возврата команд Антивируса.

Таблица 22. Команды Антивируса

Команда	Описание
KAVSHELL HELP (см. п. 16.1 на стр. 247)	Вызывает справку о командах Антивируса
KAVSHELL START (см. п. 16.2 на стр. 248)	Запускает службу Антивируса
KAVSHELL STOP (см. п. 16.2 на стр. 248)	Останавливает службу Антивируса
KAVSHELL SCAN (см. п. 16.3 на стр. 248)	Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами команды
KAVSHELL FULLSCAN (см. п. 16.4 на стр. 253)	Запускает системную задачу **Полная проверка компьютера**
KAVSHELL TASK (см. п. 16.5 на стр. 254)	Запускает / приостанавливает / возобновляет/останавливает указанную задачу в асинхронном режиме / возвращает текущее состояние задачи / статистику задачи
KAVSHELL RTP (см. п. 16.6 на стр. 255)	Запускает или останавливает все задачи постоянной защиты
KAVSHELL UPDATE (см. п. 16.7 на стр. 256)	Запускает задачу обновления баз Антивируса с параметрами, указанными с помощью ключей команды
KAVSHELL ROLLBACK (см. п. 16.8 на стр. 261)	Откатывает базы до предыдущей версии
KAVSHELL LICENSE (см. п. 16.9 на стр. 261)	Управляет лицензионными ключами
KAVSHELL TRACE (см. п. 16.10 на стр. 262)	Включает или выключает запись журнала трассировки, управляет параметрами журнала трассировки
KAVSHELL DUMP (см. п. 16.11 на стр. 264)	Включает или выключает создание дампов памяти процессов Антивируса при аварийном завершении процессов

Команда	Описание
KAVSHELL IMPORT (см. п. 16.12 на стр. 265)	Импортирует общие параметры Антивируса, параметры его функций и задач из предварительно созданного конфигурационного файла
KAVSHELL EXPORT (см. п. 16.13 на стр. 266)	Экспортирует все параметры Антивируса и существующих задач в конфигурационный файл

16.1. Вызов справки о командах Антивируса. KAVSHELL HELP

Чтобы получить список всех команд Антивируса, введите одну из следующих команд:

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

Чтобы получить описание и систаксис команды, введите одну из следующих команд:

```
KAVSHELL HELP <команда>
KAVSHELL <команда> /?
```

Примеры команды KAVSHELL HELP

`KAVSHELL HELP SCAN` – просмотреть подробную информацию о команде KAVSHELL SCAN.

16.2. Запуск и остановка службы Антивируса. KAVSHELL START, KAVSHELL STOP

Чтобы запустить службу Антивируса, используйте команду KAVSHELL START.

Примечание

По умолчанию при запуске Антивируса запускаются задачи **Постоянная защита файлов**, **Проверка скриптов**, **Проверка при старте системы** и **Проверка целостности приложения**, а также другие задачи, в расписании которых указана частота запуска **При запуске приложения**.

Чтобы остановить службу Антивируса, используйте команду KAVSHELL STOP.

16.3. Проверка указанной области. KAVSHELL SCAN

Чтобы запустить задачу проверки отдельных областей защищаемого сервера, используйте команду KAVSHELL SCAN. Ключи этой команды задают параметры задачи (область проверки и параметры безопасности).

Задача проверки по требованию, запущенная с помощью команды KAVSHELL SCAN, является *временной*. Она отображается в консоли Антивируса в MMC только во время ее выполнения (в консоли Антивируса вы не можете просматривать параметры задачи). Одновременно регистрируется отчет о выполнении задачи; он отображается в узле **Отчеты** консоли Антивируса. Так же как и к задачам проверки по требованию, созданным в консоли Антивируса, к задачам, созданным и запущенным с помощью команды SCAN, могут применяться политики приложения Kaspersky Administration Kit (информацию об использовании Kaspersky Administration Kit для управления Антивирусом содержит Часть 3 на стр. 273).

Команда KAVSHELL SCAN выполняется в синхронном режиме.

Указывая пути в задаче проверки по требованию, вы можете использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполняйте команду KAVSHELL SCAN с правами этого пользователя.

Чтобы запустить из командной строки существующую задачу проверки по требованию, используйте команду KAVSHELL TASK (см. п. 16.5 на стр. 254).

Синтаксис команды KAVSHELL SCAN

```
KAVSHELL SCAN <области проверки>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP]
[/L:< имя файла со списком областей проверки >] [/F<A|C|E>]
[/NEWONLY] [/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE]
[/E:<ABMSPO>] [/EM:<”маски”>] [/ES:<размер>]
[/ET:<количество секунд>] [/NOICHECKER][/NOISWIFT][/W:<имя
файла отчета>] [/ALIAS:<альтернативное имя задачи>]
```

Примеры команды KAVSHELL SCAN

```
KAVSHELL SCAN Folder4 D:\Folder1\Folder2\Folder3\
C:\Folder1\ C:\Folder2\3.exe “\\server1\Shared Folder\”
F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
/E:ABM /EM:”*.xtx;*.ff?;*.ggg;*.bbb;*.info” /NOICHECKER
/NOISWIFT /W:report.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:report.log
```

Ключ	Описание
Область проверки. Обязательный ключ.	
<файлы>	Область проверки – список файлов, папок, сетевых путей и предопределенных областей. Указывайте сетевые пути в формате UNC (Universal Naming Convention). В следующем примере папка Folder4 указана без пути к ней – она находится в папке, из которой вы запускаете команду KAVSHELL: KAVSHELL SCAN Folder4
<папки>	
<сетевой путь>	
/MEMORY	Проверять объекты в оперативной памяти.
/SHARED	Проверять папки общего доступа на сервере.
/STARTUP	Проверять объекты автозапуска.
/REMDRIVES	Проверять съемные диски.
/FIXDRIVES	Проверять жесткие диски.
/MYCOMP	Проверять все области защищаемого сервера.

Ключ	Описание

/L: <имя файла со списком областей проверки>	Имя файла со списком областей проверки, включая полный путь к файлу.
	Разделяйте области проверки в файле символом «перевод строки». Вы можете указывать предопределенные области проверки, как показано в следующем в примере файла со списком областей проверки:
	`C:\`
	`D:\Docs\*.doc`
	`E:\My Documents`
	`/STARTUP`
	`/SHARED`

Проверяемые объекты (File types). Если вы не зададите никаких значений этого ключа, Антивирус будет проверять объекты по формату.	
/FA	Проверять все объекты
/FC	Проверять объекты по формату (по умолчанию). Антивирус проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам.
/FE	Проверять объекты по расширению. Антивирус проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам.
/NEWONLY	Проверять только новые и измененные объекты (подробнее о параметре читайте в п. A.3.2 на стр. 400) Если вы не укажете этот ключ, Антивирус будет проверять все объекты.
/AI: **Действия над зараженными объектами**. Если вы не зададите никаких значений этого ключа, Антивирус будет выполнять действие **Пропускать**.	
DISINFECT	Лечить, если невозможно, пропускать
DISINFDEL	Лечить, если невозможно, удалять
DELETE	Удалять
REPORT	Пропускать (по умолчанию)

Ключ	**Описание**
AUTO	Выполнять рекомендованное действие
/AS: **Действия над подозрительными объектами** (actions). Если вы не зададите никаких значений этого ключа, Антивирус будет выполнять действие **Пропускать**.	
QUARANTINE	Помещать на карантин
DELETE	Удалять
REPORT	Пропускать (по умолчанию)
AUTO	Выполнять рекомендованное действие
Исключения (Exclusions)	
/E:ABMSPO	Ключ исключает составные объекты следующих типов: A – архивы; B – почтовые базы; M – файлы почтовых форматов; S – SFX-архивы; P – упакованные объекты; O – вложенные OLE-объекты.
/EM:<”маски”>	Исключать файлы по маске Вы можете задать несколько масок, например, EM:”*.txt;*.pn?; C\Videos*.avi”.
/ET:<количество секунд>	Прекращать обработку объекта, если она продолжается дольше указанного количества секунд По умолчанию ограничений в продолжительности проверки нет.
/ES:<размер>	Исключать из проверки составные объекты, размер которых в мегабайтах превышает указанный значением <размер> По умолчанию Антивирус проверяет объекты любого размера.

Ключ	Описание
Дополнительные параметры (Options)	
/NOICHECKER	Выключить использование технологии iChecker (по умолчанию включено).
/NOISWIFT	Выключить использование технологии iSwift (по умолчанию включено).
/ALIAS:<альтернативное имя задачи>	Ключ позволяет присвоить задаче проверки по требованию временное имя, по которому к задаче можно обращаться во время ее выполнения, например, чтобы просмотреть ее статистику с помощью команды TASK. Альтернативное имя задачи должно быть уникальным среди альтернативных имен задач всех функциональных компонентов Антивируса. Если этот ключ не задан, задаче присваивается альтернативное имя scan_<kavshell_pid>, например, scan_1234. В консоли Антивируса задаче присваивается имя Scan objects (<дата и время>), например, Scan objects 8/16/2007 5:13:14 PM.
Параметры отчетов (Report settings)	
/W:<имя файла отчета>	Если вы укажете этот ключ, Антивирус сохранит файл отчета о задаче с именем, заданным значением ключа. Файл отчета содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В отчете регистрируются события, заданные параметрами отчетов и журнала событий в консоли Антивируса (подробнее читайте в п. 13.2.7 на стр. 215). Вы можете указать как абсолютный, так и относительный путь к файлу отчета. Если вы укажите только имя файла, не указав путь к нему, файл отчета будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в отчет перезаписывает существующий отчет. Вы можете просматривать файл отчета по время выполнения задачи. Отчет о задаче отображается также в узле **Отчеты** консоли Антивируса.

Ключ	Описание
	Если Антивирусу не удается создать файл отчета, он не прерывает выполнение команды и не отображает сообщение об ошибке.

16.4. Запуск задачи *Полная проверка компьютера*. KAVSHELL FULLSCAN

Используйте команду KAVSHELL FULLSCAN, чтобы запустить системную задачу проверки по требованию **Полная проверка компьютера** с параметрами, заданными в консоли Антивируса в MMC.

Указывая пути в задаче проверки по требованию, вы можете использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполняйте команду KAVSHELL SCAN с правами этого пользователя.

Синтаксис команды KAVSHELL FULLSCAN

```
KAVSHELL FULLSCAN [/W:<имя файла отчета>]
```

Примеры команды KAVSHELL FULLSCAN

`KAVSHELL FULLSCAN /W:fullscan.log` – выполнить задачу проверки по требованию **Полная проверка компьютера**; отчет о событиях задачи сохранить в файле fullscan.log в текущей папке.

Ключ	Описание
/W:<имя файла отчета>	Если вы укажете этот ключ, Антивирус сохранит файл отчета о задаче с именем, заданным значением ключа. Файл отчета содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В отчете регистрируются события, заданные параметрами отчетов и журнала событий в консоли Антивируса (подробнее читайте в п. 13.2.7 на стр. 215). Вы можете указать как абсолютный, так и относительный путь к файлу отчета. Если вы укажите только имя файла отчета, не указав путь к нему, то файл

Ключ	Описание
	отчета будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в отчет перезаписывает существующий файл отчета. Вы можете просматривать файл отчета по время выполнения задачи. Отчет о задаче отображается также в узле **Отчеты** консоли Антивируса. Если Антивирусу не удается создать файл отчета, он не прерывает выполнение команды и не отображает сообщение об ошибке.

16.5. Управление указанной задачей в асинхронном режиме. KAVSHELL TASK

С помощью команды KAVSHELL TASK вы можете управлять указанной задачей: запускать, приостанавливать, возобновлять и останавливать задачу, а также просматривать ее текущее состояние и статистику. Команда выполняется в асинхронном режиме.

Синтаксис команды KAVSHELL TASK

```
KAVSHELL TASK [<альтернативное имя задачи> </START | /STOP
| /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Примеры команды KAVSHELL TASK

```
KAVSHELL TASK
KAVSHELL TASK on-access /START
KAVSHELL TASK user-task_1 /STOP
KAVSHELL TASK scan-computer /STATE
```

Ключ	Описание
Без ключей	Команда возвращает список всех существующих задач Антивируса. Список содержит поля: альтернативное имя задачи, категория задачи (системная, пользовательская или групповая) и текущее состояние задачи.

Ключ	Описание
<альтернативное имя задачи>	Вместо имени задачи в команде SCAN TASK используйте ее альтернативное имя (Task alias) – дополнительное, краткое имя, которое присваивает задачам Антивирус. Чтобы просмотреть альтернативные имена задач Антивируса, введите команду KAVSHELL TASK без ключей.
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/PAUSE	Приостановить указанную задачу
/RESUME	Возобновить указанную задачу в асинхронном режиме
/STATE	Получить текущее состояние задачи (*Выполняется*, *Завершена*, *Приостановлена*, *Остановлена, Завершена с ошибкой*, *Запускается*, *Восстанавливается*)
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи по текущий момент.

16.6. Запуск и остановка задач постоянной защиты. KAVSHELL RTP

С помощью команды KAVSHELL RTP вы можете запустить или остановить все задачи постоянной защиты.

Синтаксис команды KAVSHELL RTP

```
KAVSHELL RTP </START | /STOP>
```

Примеры команды KAVSHELL RTP

`KAVSHELL RTP /START` – запустить все задачи постоянной защиты.

Ключ	Описание
/START	Запустить все задачи постоянной защиты
/STOP	Остановить все задачи постоянной защиты

16.7. Запуск задачи обновления баз Антивируса. KAVSHELL UPDATE

С помощью команды KAVSHELL UPDATE вы можете запускать задачу обновления баз Антивируса в синхронном режиме.

Задача обновления баз Антивируса, запущенная с помощью команды KAVSHELL UPDATE, является *временной*. Она отображается в консоли Антивируса в MMC только во время ее выполнения. Одновременно регистрируется отчет о выполнении задачи; он отображается в узле **Отчеты** консоли Антивируса. К задачам обновления, созданным и запущенным с помощью команды KAVSHELL UPDATE, как и к задачам обновления, созданным в консоли Антивируса, могут применяться политики приложения Kaspersky Administration Kit (информацию об управлении Антивирусом на серверах с помощью приложения Kaspersky Administration Kit содержит Часть 3 на стр. 273).

Указывая путь к источнику обновлений в этой задаче, вы можете использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполняйте команду KAVSHELL UPDATE с правами этого пользователя.

Синтаксис команды KAVSHELL UPDATE

```
KAVSHELL UPDATE < Источник обновления | /AK | /KL>
[/NOUSEKL] [/PROXY:<адрес>:<порт>] [/AUTHTYPE:<0-2>]
[/PROXYUSER:<имя пользователя>] [/PROXYPWD:<пароль>]
[/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL]
[/NOFTPPASSIVE] [/TIMEOUT:<количество секунд>] [/REG:<код
iso3166>] [/W:<имя файла отчета>] [/ALIAS:<альтернативное
имя задачи>]
```

Примеры команды KAVSHELL UPDATE

`KAVSHELL UPDATE` – запустить пользовательскую задачу обновления баз;

`KAVSHELL UPDATE \\Server\bases` – запустить задачу обновления баз, файлы обновлений хранятся в сетевой папке \\Server\bases;

`KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com/ W:c:\update_report.log` – запустить задачу обновления с FTP-сервера ftp://dnl-ru1.kaspersky-labs.com/; записать все события задачи в файл отчета c:\update_report.log.

`KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456` – получить обновления баз Антивируса с сервера обновлений «Лаборатории Касперского»; соединиться с источником обновлений через прокси-сервер (адрес прокси-сервера: proxy.company.com, порт: 8080); для доступа к серверу использовать встроенную проверку подлинности Microsoft Windows (NTLM-authentication) под учетной записью (имя пользователя: inetuser, пароль: 123456).

Ключ	**Описание**
Источники обновления (обязательный ключ). Укажите один или несколько источников. Антивирус будет обращаться к источникам в порядке их перечисления. Разделяйте источники символом пробела.	
<путь в формате UNC>	Пользовательский источник обновлений – путь к сетевой папке с обновлениями в формате UNC (Universal Naming Convention).
<URL>	Пользовательский источник обновлений – адрес HTTP- или FTP-сервера, на котором помещается папка с обновлениями
<Локальная папка>	Пользовательский источник обновлений – папка на защищаемом сервере
/AK	Сервер администрирования Kaspersky Administration Kit в качестве источника обновлений
/KL	Серверы обновлений «Лаборатории Касперского» в качестве источника обновлений
/NOUSEKL	Не использовать серверы обновлений «Лаборатории Касперского», если другие указанные источники обновлений недоступны (по умолчанию используются)
Параметры прокси-сервера	
/PROXY:<адрес>:<порт>	Сетевое имя или IP-адрес прокси-сервера и его порт. Если вы не укажете этот ключ, Антивирус будет автоматически распознавать параметры прокси-сервера, который используется в локальной сети.

Ключ	Описание
/AUTHTYPE:<0-2>	Этот ключ задает метод проверки подлинности для доступа к прокси-серверу. Он может принимать следующие значения: **0** – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Антивирус будет обращаться к прокси-серверу под учетной записью **Локальная система** (**SYSTEM**); **1** – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Антивирус будет обращаться к прокси-серверу под учетной записью, данные которой описаны ключами /PROXYUSER и /PROXYPWD; **2** – проверка подлинности по имени и паролю пользователя, заданным ключами /PROXYUSER и /PROXYPWD (Basic authentication). Если для доступа к прокси-серверу не требуется проверка подлинности, то указывать этот ключ нет необходимости.
/PROXYUSER:<имя пользователя>	Имя пользователя, которое будет использоваться для доступа к прокси-серверу. Если вы укажете значение ключа /AUTHTYPE:0, то ключи /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются.
/PROXYPWD:<пароль>	Пароль пользователя, который будет использоваться для доступа к прокси-серверу. Если вы укажете значение ключа /AUTHTYPE:0, то ключи /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются. Если вы укажете ключ /PROXYUSER, а ключ /PROXYPWD опустите, то считается что пароль пустой.
/NOPROXYFORKL	Не использовать параметры прокси-сервера для соединения с серверами обновлений «Лаборатории Касперского» (по умолчанию используются)
/USEPROXYFORCUSTOM	Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений (по умолчанию не используются)

Ключ	Описание
/USEPROXYFORLOCAL	Использовать параметры прокси-сервера для соединения с локальными источниками обновлений. Если не указано, применяется значение **Не использовать настройки прокси-сервера для соединения с локальными источниками обновления**. Подробее об этих параметрах читайте в п. A.5.4.1 на стр. 429.
Общие параметры FTP- и HTTP-сервера	
/NOFTPPASSIVE	Если вы укажете этот ключ, Антивирус будет использовать активный режим FTP-сервера для соединения с защищаемым сервером. Если вы не укажете этот ключ, то Антивирус будет использовать пассивный режим FTP-сервера, если возможно.
/TIMEOUT:<количество секунд>	Время ожидания при соединении с FTP- или HTTP-сервером. Если вы не укажете этот ключ, Антивирус будет использовать значение по умолчанию: 10 сек. В качестве значения ключа вы можете вводить только целые числа.
/REG:<код iso3166>	Ключ «Региональные настройки» используется при получении обновлений с серверов обновлений «Лаборатории Касперского». Антивирус оптимизирует загрузку обновлений на защищаемый сервер, выбирая ближайший к нему сервер обновлений. В качестве значения ключа укажите буквенный код страны местоположения защищаемого сервера в соответствии со стандартом ISO 3166-1, например, /REG:gr или /REG:RU. Если вы опустите этот ключ или укажете несуществующий код страны, то Антивирус будет распознавать местоположение защищаемого сервера в соответствии с региональными настройками защищаемого сервера (для Microsoft Windows 2003 Server и выше – по значению переменной **Расположение** (**Location**)).

Ключ	Описание
/ALIAS:<альтернативное имя задачи>	Этот ключ позволяет присвоить задаче временное имя, по которому к ней можно обращаться во время ее выполнения. Например, вы можете просмотреть статистику задачи с помощью команды TASK. Альтернативное имя задачи должно быть уникальным среди альтернативных имен задач всех функциональных компонентов Антивируса. Если этот ключ не задан, задаче приваивается альтернативное имя update_<kavshell_pid>, например, update_1234. В консоли Антивируса задаче присваивается имя Update-bases (<date time>), например, Update-bases 8/16/2007 5:41:02 PM.
/W:<имя файла отчета>	Если вы укажете этот ключ, Антивирус сохранит файл отчета о задаче с именем, заданным значением ключа. Файл отчета содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В отчете регистрируются события, заданные параметрами отчетов и журнала событий в консоли Антивируса (подробнее читайте в п. 13.2.7 на стр. 215). Вы можете указать как абсолютный, так и относительный путь к файлу отчета. Если вы укажите только имя файла отчета, не указав путь к нему, то файл отчета будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в отчет перезаписывает существующий файл отчета. Вы можете просматривать файл отчета во время выполнения задачи. Отчет о задаче отображается также в узлах **Отчеты** консоли Антивируса. Если Антивирусу не удается создать файл отчета, он не прерывает выполнение команды и не отображает сообщение об ошибке.

16.8. Откат обновления баз Антивируса. KAVSHELL ROLLBACK

С помощью команды KAVSHELL ROLLBACK вы можете выполнить системную задачу **Откат обновления баз** – откатить базы Антивируса до предыдущих установленных обновлений. Команда выполняется синхронно.

Синтаксис команды

```
KAVSHELL ROLLBACK
```

16.9. Установка и удаление ключей. KAVSHELL LICENSE

С помощью команды KAVSHELL LICENSE вы можете устанавливать и удалять ключи Антивируса.

Синтаксис команды KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<имя файла ключа> [/R] |
/DEL:<серийный номер>]
```

Примеры команды KAVSHELL LICENSE

`KAVSHELL LICENSE /ADD:C:/License.key` – установить ключ из файла;

`KAVSHELL LICENSE` – получить информацию об установленных ключах;

`KAVSHELL LICENSE /DEL:0000-000000-00000001` – удалить установленный ключ с серийным номером 0000-000000-00000001.

Ключ	Описание
Без ключей	Команда возвращает следующую информацию об установленных ключах: • серийный номер ключа; • тип ключа (для бета-тестирования, коммерческий или пробный); • срок действия ключа; • является ли ключ резервным. Если указано значе-

Ключ	Описание
	ние *, то ключ установлен в качестве резервного.
/ADD:<имя файла ключа>	Устанавливает ключ из файла с именем, заданным значением /ADD. Включите имя файла ключа и полный путь к нему. Указывая путь к файлу ключа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/R	Ключ /R является дополнительным к ключу /ADD. Он указывает на то, что устанавливаемый ключ является резервным.
/DEL:<серийный номер>	Удаляет ключ с серийным номером, заданным значением /DEL.

16.10. Включение, настройка и выключение создания журнала трассировки. KAVSHELL TRACE

С помощью команды KAVSHELL TRACE вы можете «на лету» включать или выключать ведение журнала трассировки всех подсистем Антивируса, а также устанавливать уровень детализации информации в журнале.

Синтаксис команды KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<папка с файлами журнала трассировки> [/S:<максимальный размер файла журнала в мегабайтах>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

Если журнал трассировки ведется и вы хотите изменить его параметры, то введите команду KAVSHELL TRACE с ключом /ON и задайте параметры журнала значениями ключей /S и /LVL.

Ключ	Описание
/ON	Включить ведение журнала трассировки
/F:<папка с файлами журнала трассировки>	Этот ключ указывает полный путь к папке, в которой будут сохранены файлы журнала трассировки (обязательный ключ). Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Вы можете указывать сетевые пути в формате UNC (Universal Naming Convention), но не можете указывать пути к папкам на сетевых дисках защищаемого сервера. Если имя папки, путь к которой вы указываете в качестве значения ключа, содержит символ пробела, заключите этот путь в кавычки, например, /F:"C\Trace Folder". Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/S:<максимальный размер файла журнала в мегабайтах>	Этот ключ устанавливает максимальный размер одного файла журнала трассировки. Как только файл журнала достигнет максимального размера, Антивирус начнет записывать информацию в новый файл; предыдущий файл журнала сохранится. Если вы не укажете этот ключ, то максимальный размер одного файла журнала составит 50МБ.
/LVL:debug|info|warning|error|critical	Этот ключ устанавливает уровень детализации журнала от максимального (*Отладочная информация*), при котором в журнал записываются все события, до минимального (*Критические*), при котором в журнал записываются только критические события. Если вы не укажете этот ключ, то в журнал трассировки будут записываться события с уровнем детализации *Отладочная информация*.
/OFF	Этот ключ выключает ведение журнала трассировки.

Примеры команды KAVSHELL TRACE:

`KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200` – включить ведение журнала трассировки с уровнем детализации *Отладочная информа-*

ция и максимальным размером файла журнала 200МБ; сохранить файл журнала в папке C:\Trace Folder.

`KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning` – включить ведение журнала трассировки с уровнем детализации *Важные события*; сохранить файл журнала в папке C:\Trace Folder:

`KAVSHELL TRACE /OFF` – выключить ведение журнала трассировки.

16.11. Включение и выключение создания файлов дампов. KAVSHELL DUMP

С помощью команды KAVSHELL DUMP вы можете «на лету» включать или выключать создание образов памяти (дампов) процессов Антивируса при их аварийном завершении. Кроме этого вы можете в любой момент снять образы памяти выполняющихся процессов Антивируса.

Синтаксис команды KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<папка с файлами дампов>|/SNAPSHOT
/F:<папка с файлами дампов> / P:<pid> | /OFF>
```

Примеры команды KAVSHELL DUMP

`KAVSHELL DUMP /ON /F:"C:\Dump Folder"` – включить создание дампов; сохранять файлы дампов в папку C:\Dump Folder;

`KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234` – снять дамп памяти процесса с идентификатором 1234 в папку C:/Dumps.

`KAVSHELL DUMP /OFF` – выключить создание дампов.

Ключ	Описание
/ON	Включает воздание дампов памяти процесса при его аварийном завершении.

Ключ	Описание
/F:<папка с файлами дампов>	Обязательный ключ; указывает путь к папке, в которой будет сохранен файл дампов. Если вы укажете путь к несуществующей папке, то файл дампов не будет создан. Вы можете использовать сетевые пути в формате UNC (Universal Naming Convention), но не можете указывать пути к папкам на сетевых дисках защищаемого сервера. Указывая путь к папке с файлами дампов, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/SNAPSHOT	Снимает образ памяти указанного выполняющегося процесса Антивируса и сохраняет файл дампа в папке, путь к которой указан ключом /F.
/P	Идентификатор PID процесса; отображается в Диспетчере задач Microsoft Windows
/OFF	Выключает создание дампов памяти процессов при аварийном завершении

16.12. Импорт параметров. KAVSHELL IMPORT

С помощью команды KAVSHELL IMPORT вы можете импортировать параметры Антивируса, его функций и задач из конфигурационного файла в Антивирус на защищаемом сервере. Вы можете создать конфигурационный файл с помощью команды KAVSHELL EXPORT.

Синтаксис команды KAVSHELL IMPORT

```
KAVSHELL IMPORT <имя конфигурационного файла и путь к файлу>
```

Примеры команды KAVSHELL IMPORT

```
KAVSHELL IMPORT Server1.xml
```

Ключ	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, из которого будут импортированы параметры. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

16.13. Экспорт параметров. KAVSHELL EXPORT

С помощью команды KAVSHELL EXPORT вы можете экспортировать все параметры Антивируса и существующих задач в конфигурационный файл, чтобы потом импортировать их в Антивирус на других серверах.

Синтаксис команды KAVSHELL EXPORT

```
KAVSHELL EXPORT <имя конфигурационного файла и путь к файлу>
```

Примеры команды KAVSHELL EXPORT

```
KAVSHELL EXPORT Server1.xml
```

Ключ	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, в котором будут сохранены параметры. Вы можете присвоить конфигурационному файлу любое расширение. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

ГЛАВА 17. КОДЫ ВОЗВРАТА

В следующих таблицах описаны коды возврата команд Антивируса.

Коды возврата команд KAVSHELL SCAN и KAVSHELL FULLSCAN

Код возврата	Описание
0	Операция выполнена успешно (Угроз не обнаружено)
1	Операция отменена
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден файл со списком областей проверки)
-5	Неверный синтаксис команды или не определена область проверки
-80	Обнаружены зараженные объекты
-81	Обнаружены подозрительные объекты
-82	Обнаружены ошибки обработки
-83	Обнаружены непроверенные объекты
-84	Обнаружены поврежденные объекты
-99	Неизвестная ошибка
-301	Недействительный ключ

Коды возврата команд KAVSHELL START и KAVSHELL STOP

Код возврата	Описание
0	Операция выполнена успешно
-3	Ошибка прав доступа
-5	Неверный синтаксис команды

Код возврата	Описание
-6	Неверная операция (например, служба Антивируса уже запущена или уже остановлена)
-7	Служба не зарегистрирована
-8	Запуск службы запрещен
-9	Попытка запустить службу под другой учетной записью не была успешной (по умолчанию служба Антивируса работает под учетной записью **Локальная система**).
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL TASK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (задача не найдена)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача не запущена, уже запущена или не может быть приостановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ
401	Задача не запущена (для ключа /STATE)
402	Задача уже запущена (для ключа /STATE)
403	Задача уже приостановлена (для ключа /STATE)
-404	Ошибка выполнения операции (изменение состояния задачи привело ее к сбою)

Коды возврата команды KAVSHELL LICENSE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Недостаточно прав для управления ключами
-4	Объект на найден (ключ с указанным серийным номером не найден)
-5	Неверный синтаксис команды
-6	Неверная операция (ключ уже установлен)
-99	Неизвестная ошибка
-301	Недействительный ключ
-303	Ключ для другого приложения

Коды возврата команды KAVSHELL UPDATE

Код возврата	Описание
0	Операция выполнена успешно
200	Все объекты актуальны (базы или программные компоненты в актуальном состоянии)
-2	Служба не запущена
-3	Ошибка прав доступа
-5	Неверный синтаксис команды
-99	Неизвестная ошибка
-206	Файлы обновлений отсутствуют в указанном источнике или имеют неизвестный формат
-209	Ошибка подключения к источнику обновлений
-232	Антивирус не прошел проверку подлинности при соединении с прокси-сервером

Код возврата	Описание
-234	Ошибка подключения к приложению Kaspersky Administration Kit
-235	Антивирус не прошел проверку подлинности при соединении с источником обновлений
-301	Недействительный ключ

Коды возврата команды KAVSHELL ROLLBACK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-99	Неизвестная ошибка
-221	Резервная копия баз не найдена
-222	Резервная копия баз повреждена

Коды возврата команды KAVSHELL RTP

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найдена какая-либо из задач постоянной защиты или все задачи постоянной защиты)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача уже запущена или уже остановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ

Коды возврата команды KAVSHELL DUMP

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден путь, указанный с качестве пути к папке с файлами дампов; не найден процесс с указанным PID)
-5	Неверный синтаксис команды
-6	Неверная операция (попытка выполнения KAVSHELL DUMP /OFF, если создание файлов дампов уже выключено)
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL TRACE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден путь, указанный в качестве пути к папке с файлами журнала трассировки)
-5	Неверный синтаксис команды
-6	Неверная операция (попытка выполнения KAVSHELL TRACE /OFF, если создание журнала трассировки уже выключено)
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL IMPORT

Код возврата	Описание
0	Операция выполнена успешно

Код возврата	Описание
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден импортируемый конфигурационный файл)
-5	Неверный синтаксис
-99	Неизвестная ошибка
501	Операция выполнена успешно; однако во время выполнения команды возникла ошибка / замечание, например, Антивирус не импортировал параметры какого-либо из функциональных компонентов
-502	Импортируемый файл отсутствует или имеет неизвестный формат
-503	Несовместимые параметры (конфигурационный файл экспортирован из другого приложения или Антивируса более поздней или несовместимой версии)

Коды возврата команды KAVSHELL EXPORT

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-5	Неверный синтаксис
-10	Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу)
-99	Неизвестная ошибка
501	Операция выполнена успешно, однако во время выполнения команды возникла ошибка / замечание, например, Антивирус не экспортировал параметры какого-либо из функциональных компонентов

ЧАСТЬ 3. НАСТРОЙКА И УПРАВЛЕНИЕ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

Если в вашей организации используется Kaspersky Administration Kit для централизованного управления антивирусными приложениями, то вы можете управлять Антивирусом на защищаемых серверах и настраивать его через Консоль администрирования Kaspersky Administration Kit.

В этой части содержится следующая информация:

- управление Антивирусом и просмотр его состояния (Глава 18 на стр. 274);
- создание и настройка политик (Глава 19 на стр. 284);
- настройка Антивируса в диалоговом окне **Параметры приложения** (Глава 20 на стр. 297);
- создание и настройка задач (Глава 21 на стр. 331).

ГЛАВА 18. УПРАВЛЕНИЕ АНТИВИРУСОМ И ПРОСМОТР ЕГО СОСТОЯНИЯ

В этой главе содержится следующая информация:

- запуск и остановка службы Антивируса (см. п. 18.1 на стр. 274);
- просмотр состояния защиты сервера (см. п. 18.2 на стр. 275);
- просмотр статистики Антивируса (см. п. 18.3 на стр. 278);
- просмотр информации об Антивирусе (см. п. 18.4 на стр. 280);
- просмотр информации об установленных ключах (см. п. 18.5 на стр. 281).

18.1. Запуск и остановка службы Антивируса

Служба Антивируса запускается автоматически при старте операционной системы. Эта служба управляет рабочими процессами, в которых выполняются задачи постоянной защиты, проверки по требованию и обновления.

По умолчанию при запуске службы Антивируса запускаются задачи **Постоянная защита файлов**, **Проверка скриптов**, **Проверка при старте системы** и **Проверка целостности приложения**, а также другие задачи, в расписании которых указана частота запуска **При запуске приложения**.

Если вы остановите службу Антивируса, выполнение всех задач будет прервано. После того как вы снова запустите службу Антивируса, прерванные задачи не будут автоматически возобновлены. Только задачи, в расписании которых указана частота запуска **При запуске приложения**, будут запущены заново.

Чтобы запустить или остановить службу Антивируса:

1. В дереве Консоли администрирования разверните узел **Группы** и выберите группу, к которой принадлежит защищаемый сервер.

2. В панели результатов откройте контекстное меню на строке с информацией о защищаемом сервере и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: <Имя компьютера>** на закладке **Приложения** выберите команду **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** в списке установленных приложений и нажмите на кнопку **Свойства**.
4. В диалоговом окне **Параметры приложения** откройте закладку **Общие**.
5. Выполните одно из следующих действий:
   - чтобы запустить службу Антивируса, нажмите на кнопку **Запустить**;
   - чтобы остановить службу Антивируса, нажмите на кнопку **Остановить**.
6. Нажмите на кнопку **ОК**.

18.2. Просмотр состояния защиты сервера

В Консоли администрирования вы можете просматривать состояние защиты выбранного сервера: состояние задач **Постоянная защита файлов** и **Проверка скриптов**, общий статус сервера с точки зрения антивирусной безопасности и его доступность.

Чтобы просмотреть состояние защиты выбранного сервера:

1. В дереве Консоли администрирования разверните узел **Группы** и выберите группу, к которой принадлежит защищаемый сервер.
2. В панели результатов откройте контекстное меню на строке с информацией о защищаемом сервере и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: <Имя компьютера>** откройте закладку **Защита** (см. рис. 93).

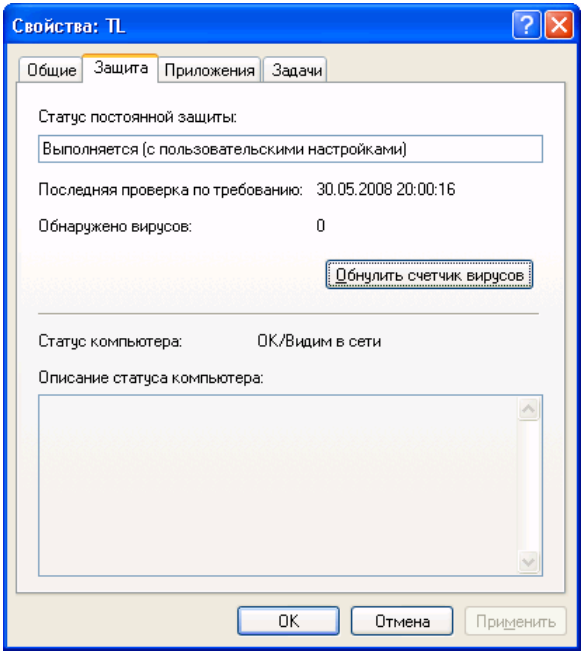

Рисунок 93. Диалоговое окно **Свойства: <Имя компьютера>**, закладка **Защита**

На закладке **Защита** отображается следующая информация о защищаемом сервере:

Таблица 23. Информация о защищаемом сервере на закладке **Защита**

Поле	Описание
Статус постоянной защиты	Показывает состояние постоянной защиты: **Выполняется** – если выполняется задача **Постоянная защита файлов** или задача **Проверка скриптов**. Если выполняется задача **Постоянная защита файлов**, статус постоянной защиты отображает название применяемого в задаче уровня безопасности: • **Рекомендуемый** – параметры безопасности в задаче соответствуют предустановленному уровню **Рекомендуемый**; • **Максимальная защита** – параметры безопасности в задаче соответствуют предустановленному уровню **Максимальная защита**; • **Максимальная скорость** – параметры безопасности в задаче соответствуют предустановленному уровню **Максимальная скорость**. • **С пользовательскими настройками** – параметры безопасности, указанные в задаче, соответствуют уровню безопасности **Другой**. Подробнее о предустановленных уровнях безопасности читайте в п. 6.2.2.1 на стр. 78.
Последняя проверка по требованию	Дата и время последнего выполнения задачи проверки по требованию, которая имеет статус «Задача полной проверки компьютера».
Обнаружено вирусов	Общее количество вредоносных программ (названий угроз), обнаруженных на защищаемом сервере (счетчик обнаруженных угроз) с момента установки Антивируса или с момента сброса счетчика. Чтобы сбросить счетчик, нажмите на кнопку **Обнулить счетчик угроз**.
Статус компьютера	Статус сервера с точки зрения антивирусной безопасности. Подробее о статусах компьютера читайте на сайте Службы технической поддержки «Лаборатории Касперского», код статьи: **987**.

18.3. Просмотр статистики Антивируса

В Консоли администрирования вы можете просматривать статистическую информацию об Антивирусе на выбранном защищаемом сервере: количество рабочих процессов Антивируса, количество записей в установленных на сервере базах Антивируса, дату создания последних установленных обновлений баз, а также информацию о работе отдельных функциональных компонентов Антивируса и выполнении задач.

Примечание

Если вы хотите просматривать статистику Антивируса в реальном времени, откройте порт UDP 15000 в брандмауэре Windows компьютера, на котором установлен Сервер администрирования.

Чтобы просмотреть статистику Антивируса:

1. В дереве Консоли администрирования разверните узел **Группы** и выберите группу, к которой принадлежит защищаемый сервер.
2. В панели результатов откройте контекстное меню на строке с информацией о защищаемом сервере и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: <Имя компьютера>** на закладке **Приложения** выберите команду **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** в списке установленных антивирусных приложений и нажмите на кнопку **Статистика**. Откроется диалоговое окно **Статистика** (см. рис. 94).

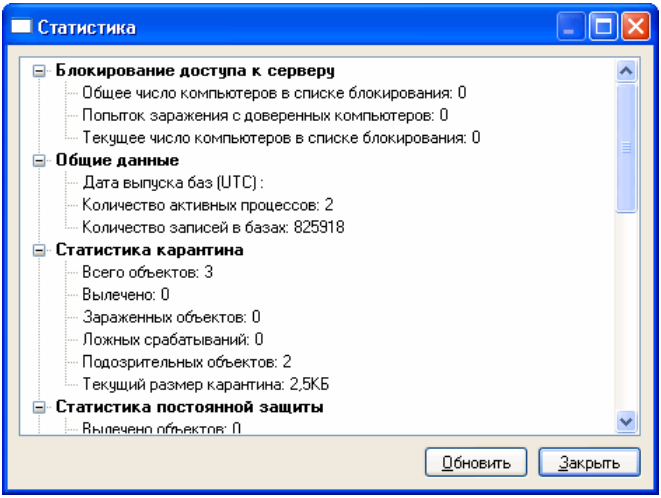

Рисунок 94. Диалоговое окно **Статистика**

В диалоговом окне **Статистика** отображается следующая информация:

Таблица 24. Информация о состоянии Антивируса на защищаемом сервере

Поле	Описание
Дата создания баз (UTC)	Дата и время создания «Лабораторией Касперского» последних установленных обновлений баз в формате UTC (Coordinated Universal Time)
Количество активных процессов	Количество рабочих процессов Антивируса, в которых в текущий момент выполняются задачи постоянной защиты, проверки по требованию и обновления
Количество записей в базах	Общее количество записей в установленных на сервере базах Антивируса
Статистика карантина	Информация о текущем состоянии карантина (подробнее читайте в п. 11.9 на стр. 187)
Статистика постоянной защиты файлов	Информация о задаче **Постоянная защита файлов** (подробнее читайте в п. 6.3 на стр. 90)

Поле	Описание
Статистика блокирования	Информация о количестве компьютеров, доступ с которых к защищаемому серверу был заблокирован с момента последнего запуска Антивируса (подробнее читайте в п. 7.9 на стр. 106)
Статистика проверки по требованию	Информация о выполняющихся задачах проверки по требованию (подробнее читайте в п. 9.4 на стр. 145)
Статистика проверки скриптов	Информация о количестве скриптов, которые Антивирус обработал с момента запуска задачи **Проверка скриптов** по текущий момент (подробнее читайте в п. 6.5 на стр. 94)
Статистика резервного хранилища	Информация о текущем состоянии резервного хранилища (подробнее читайте в п. 12.6 на стр. 201)

Примечание

Информация о задаче **Постоянная защита файлов**, **Проверка скриптов** и задачах проверки по требованию отображается только тогда, когда соответствующая задача выполняется.

18.4. Просмотр информации об Антивирусе

Вы можете просматривать информацию об Антивирусе и его базах.

Чтобы просмотреть информацию об Антивирусе:

1. В дереве Консоли администрирования разверните узел **Группы** и выберите группу, к которой принадлежит защищаемый сервер.
2. В панели результатов откройте контекстное меню на строке с информацией о защищаемом сервере и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: <Имя компьютера>** на закладке **Приложения** выберите команду **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** в списке установленных приложений и нажмите на кнопку **Свойства**.

4. В диалоговом окне **Параметры приложения** откройте закладку **Общие**.

На закладке **Общие** (см. рис. 103) отображается:

- общая информация об Антивирусе:
  - номер версии;
  - дата и время установки;
  - дата и время последнего обновления модулей Антивируса;
  - состояние службы Антивируса (запущена / остановлена);
- информация о базах Антивируса:
  - дата и время создания установленных обновлений баз (в формате, заданном региональными настройками компьютера, на котором установлена Консоль администрирования);
  - общее количество записей в базах;
  - дата и время последнего обновления.

18.5. Просмотр информации об установленных ключах

Чтобы просмотреть информацию об установленных ключах:

1. В дереве Консоли администрирования разверните узел **Группы** и выберите группу, к которой принадлежит защищаемый сервер.
2. В панели результатов откройте контекстное меню на строке с информацией о защищаемом сервере и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: <Имя компьютера>** на закладке **Приложения** выберите команду **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** в списке установленных приложений и нажмите на кнопку **Свойства**.
4. В диалоговом окне **Параметры приложения** откройте закладку **Лицензии** (см. рис. 95).

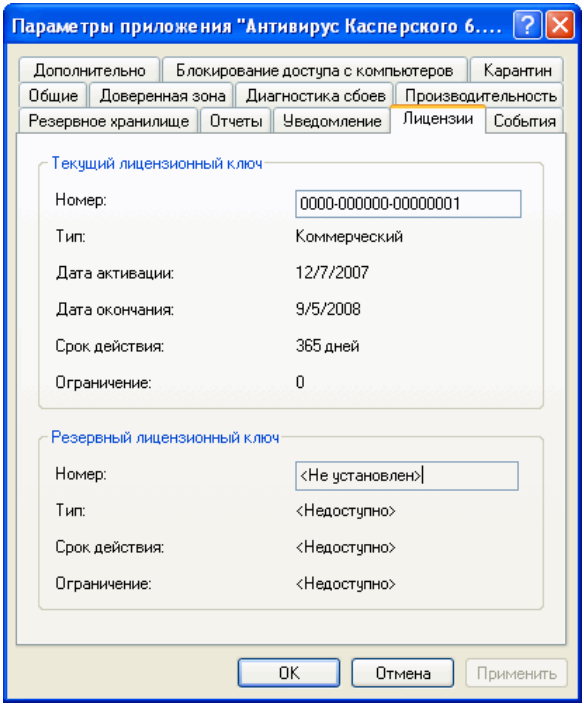

Рисунок 95. Диалоговое окно **Параметры приложения**, закладка **Лицензии**

На закладке **Лицензии** отображается следующая информация об установленных ключах:

Таблица 25. Информация об установленных ключах

Поле	Описание
Номер	Серийный номер ключа
Тип	Тип ключа (для бета-тестирования, пробный или коммерческий). Подробнее о типах ключей читайте в п. 14.1 на стр. 228.
Дата активации	Дата установки ключа (только для активного ключа)
Дата окончания	Дата окончания срока действия ключа (только для активного ключа); рассчитывается Антивирусом при установке ключа; наступает, когда за-

	вершается *период действия ключа* с момента его активации, но не позднее *даты, когда ключ становится недействительным*.
Срок действия	Количество дней до истечения срока действия ключа
Ограничение	Предусмотренное ключом ограничение (если имеется)

ГЛАВА 19. СОЗДАНИЕ И НАСТРОЙКА ПОЛИТИК

В этой главе содержится следующая информация:

- о политиках (см. п. 19.1 на стр. 284);
- создание политики (см. п. 19.2 на стр. 285);
- настройка политики (см. п. 19.3 на стр. 290);
- отключение расписания запуска локальных системных задач (см. п. 19.4 на стр. 294).

19.1. О политиках

Вы можете создавать единые политики Kaspersky Administration Kit для управления защитой нескольких серверов, на которых установлен Антивирус.

Политика применяет указанные в ней значения параметров Антивируса, его функций и задач на всех защищаемых серверах одной группы администрирования.

Примечание

С помощью политик вы не можете формировать область защиты (проверки) в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. В Консоли администрирования политика, действующая в группе в текущий момент, имеет статус *активна*.

Информация о применении политики регистрируется в журнале системного аудита Антивируса. Вы можете просмотреть ее в консоли Антивируса в ММС, в узле **Журнал системного аудита**.

Из всех способов применения политик вы можете использовать только способ **Не изменять параметры**, который не предполагает сохранения определенных политикой значений параметров в Антивирусе. Вы не можете использовать способы применения политик **Изменять обязательные параметры** и **Изменять все параметры**.

Согласно способу применения политик **Не изменять параметры**, Антивирус на время действия политики применяет значения параметров, рядом с которыми в свойствах политики вы установили значок, вместо значений этих параметров, действующих до применения политики. Антивирус не применяет значения параметров, рядом с которыми в свойствах политики установлен значок. Как только действие политики завершается, параметры, значения которых были изменены политикой, снова принимают значения, действовавшие до ее применения.

Во время действия политики в консоли Антивируса в MMC и в диалоговом окне **Свойства приложения** Консоли администрирования отображаются значения параметров, помеченные в политике значком; они не доступны для редактирования. Значения остальных параметров (которые в политике помечены значком) доступны для редактирования в консоли Антивируса в MMC и диалоговом окне **Свойства приложения** Консоли администрирования.

Если политика определяет параметры какой-либо из задач постоянной защиты и эта задача выполняется, то параметры, определенные политикой, применяются сразу, как только политика становится активной. Если задача не выполняется, то параметры применятся при ее запуске. Если политикой определяются параметры других задач Антивируса, то, когда политика становится активной, эти параметры не применяются в выполняющихся задачах, а только при последующем запуске задач.

19.2. Создание политики

Создание новой политики состоит из двух этапов:

1. Вы создаете политику с помощью мастера создания политик. В окнах мастера вы можете установить параметры задач **Обновление баз приложения**, **Обновление модулей приложения**, **Постоянная защита файлов** и **Проверка по требованию**.

2. В диалоговом окне **Свойства политики** вы, в соответствии со своими требованиями, устанавливаете параметры остальных задач и параметры Антивируса.

   В диалоговом окне **Свойства политики** вы можете изменять настроенные с помощью мастера создания политик параметры задач обновления и проверки по требованию и задачи **Постоянная защита файлов**. Подробнее о том, как настроить созданную политику, читайте в п. 19.3 на стр. 290.

Чтобы создать политику для группы серверов, на которых установлен Антивирус:

1. В дереве Консоли администрирования разверните узел **Группы**, а затем разверните группу администрирования, для серверов которой вы хотите создать политику.

2. В контекстном меню вложенного узла **Политики** выберите команду **Создать → Политику**.

   Откроется окно мастера создания политик.

3. В окне **Имя политики** в поле ввода введите имя создаваемой политики (оно не может содержать символы **“ * < : > ? \ / |**).

4. В окне **Приложения** под заголовком **Приложение** выберите **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition**.

5. В окне **Создание политики** выберите одно из следующих состояний политики:

   - **Активная политика**, если вы хотите, чтобы политика вступила в действие сразу после ее создания. Если в группе уже существует активная политика, то эта существующая политика станет неактивной, а создаваемая вами политика будет активирована.

   - **Неактивная политика**, если вы не хотите сразу применять создаваемую политику. Вы сможете активировать политику позже.

   В следующих окнах мастера создания политик установите в соответствии с вашими требованиями параметры задач **Обновление баз приложения**, **Обновление модулей приложения**, **Постоянная защита файлов** и **Проверка по требованию**.

6. В окне **Постоянная защита файлов** (см. рис. 96) выберите режим защиты объектов в задаче **Постоянная защита файлов** и выберите один из предустановленных уровней безопасности или настройте вручную параметры безопасности (см. п. A.3 на стр. 398).

   Установите флажок **Применять доверенную зону**, если в задаче **Постоянная защита файлов** вы хотите исключить из области защиты объекты, описанные в доверенной зоне Антивируса (подробнее о доверенной зоне читайте в п. 8.1 на стр. 108; о том, как добавлять исключения в доверенную зону в приложении Kaspersky Administration Kit, читайте в п. 20.7 на стр. 322).

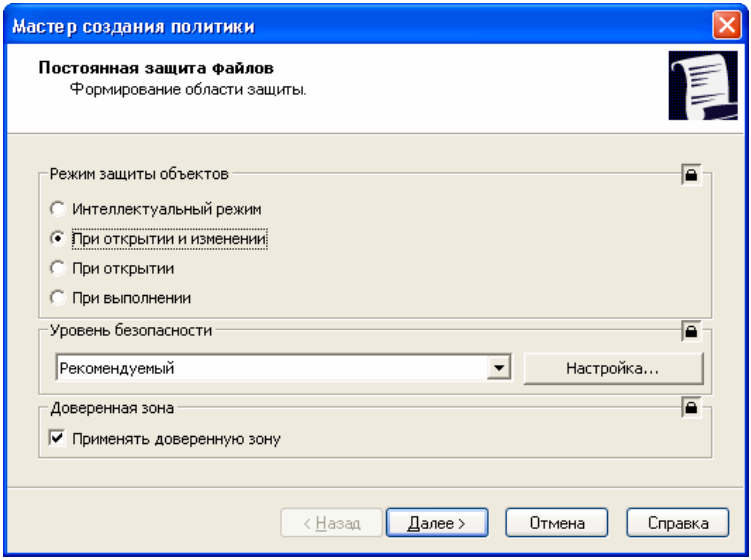

Рисунок 96. Окно **Постоянная защита файлов**

7. В окне **Проверка по требованию** (см. рис. 97) выберите один из предустановленных уровней безопасности или настройте вручную параметры безопасности в задачах проверки по требованию (см. п. A.3 на стр. 398).

   Установите флажок **Применять доверенную зону**, если в задачах проверки по требованию вы хотите исключить из области защиты объекты, описанные в доверенной зоне Антивируса (подробнее о доверенной зоне читайте в п. 8.1 на стр. 108; о том, как добавлять исключения в доверенную зону в приложении Kaspersky Administration Kit, читайте в п. 20.7 на стр. 322).

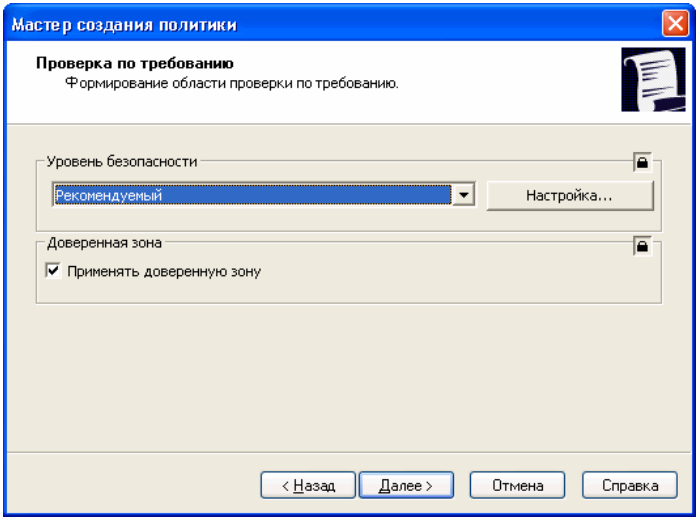

Рисунок 97. Окно **Проверка по требованию**

8. В окне **Обновление** (см. рис. 98) настройте параметры задач **Обновление баз приложения** и **Обновление модулей приложения**.

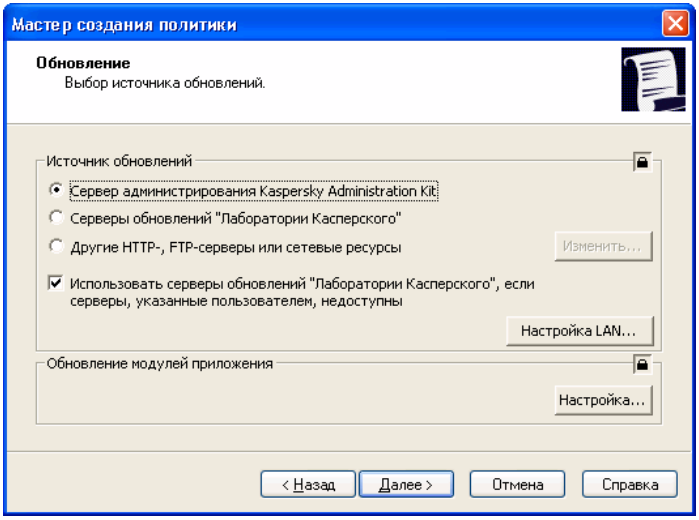

Рисунок 98. Окно **Обновление**

9. В окне **Настройка** выполните следующие действия:

   а) Выберите источник обновлений (см. п. А.5.1 на стр. 426).

   б) Нажмите на кнопку **Настройка LAN**. В диалоговом окне **Настройка соединения** настройте нужные параметры соединения:

   - измените режим FTP-сервера для соединения с защищаемым сервером и время ожидания при соединении (см. п. А.5.2 на стр. 427);
   - настройте параметры доступа к прокси-серверу при соединении с источником обновлений (см. п. А.5.4 на стр. 429);
   - на закладке **Региональные настройки** укажите местоположение защищаемого сервера (серверов), чтобы оптимизировать получение обновлений (см. п. А.5.5 на стр. 432).

   в) Чтобы настроить параметры задачи **Обновление модулей приложения**, в окне **Обновление** нажмите на кнопку **Настройка** под заголовком **Обновление модулей приложения** и в диалоговом окне **Настройка обновления модулей приложения** (см. рис. 99) настройте параметры обновления программных модулей:

   - Выберите, загружать и устанавливать обновления программных модулей или только проверять их наличие. (см. п. А.5.6.1 на стр. 433).

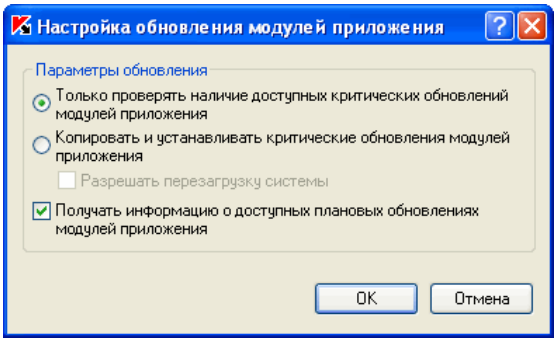

Рисунок 99. Диалоговое окно **Настройка обновления модулей приложения**

   - Чтобы после завершения задачи Антивирус автоматически запускал перезагрузку сервера, если она потребуется для применения установленных программных модулей, установите флажок **Разрешать перезагрузку системы**.

- Если вы хотите получать информацию о выходе плановых обновлений модулей антивируса, установите флажок **Получать информацию о доступных плановых обновлениях модулей приложения**.

  «Лаборатория Касперского» не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете сами загружать их с вебсайта «Лаборатории Касперского». Вы можете настроить уведомления администратора о событии *Доступно плановое обновление модулей Антивируса*, в которых будет содержаться адрес страницы на нашем сайте, откуда вы сможете загружать плановые обновления (подробнее о настройке уведомлений читайте в п. 15.2 на стр. 237).

Примечание

Параметры задачи **Копирование обновлений** вы сможете настроить позже, в диалоговом окне **Свойства политики**.

10. В окне **Завершение работы** нажмите на кнопку **Готово**.

Созданная политика отобразится в списке политик в узле **Политики** выбранной группы администрирования. Теперь в диалоговом окне **Свойства политики** вы можете настроить другие параметры Антивируса, его функций и задач.

19.3. Настройка политики

В диалоговом окне **Свойства** существующей политики вы можете настроить общие параметры Антивируса, параметры его функций и задач для серверов группы администрирования.

Примечание

С помощью политики вы не можете формировать область защиты (проверки) в задаче **Постоянная защита файлов** и задачах проверки по требованию.

*Чтобы настроить параметры в диалоговом окне **Свойства политики**:*

1. В дереве Консоли администрирования разверните узел **Группы**, разверните группу администрирования, параметры политики которой вы хотите настроить, затем разверните вложенный узел **Политики**.

2. В панели результатов откройте контекстное меню на политике, параметры которой вы хотите настроить, и выберите команду **Свойства**.

3. В диалоговом окне **Свойства: <Название политики>** (см. рис. 100) настройте нужные параметры политики.

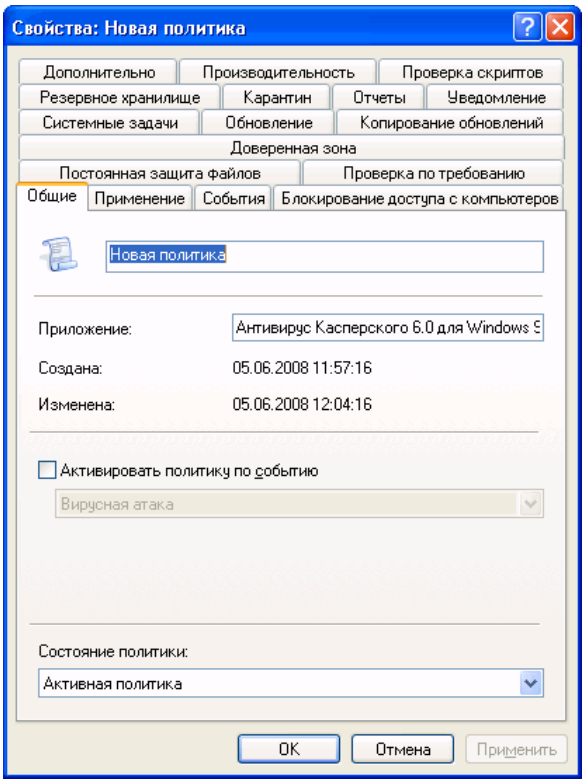

Рисунок 100. Пример диалогового окна **Свойства : <Название политики>**

Вы можете настроить параметры политики на следующих закладках:

Таблица 26. Настройка параметров политики

Параметры	Закладка
Параметры безопасности в задаче **Постоянная защита файлов**: • **режим защиты объектов** (см. описание параметра в п. A.3.1 на стр. 399); • **параметры безопасности** (единые для всей области защиты): вы можете выбрать предустановленный уровень безопасности (см. описание в п. 6.2.2.1 на стр. 78) или настроить параметры безопасности вручную (так же как в консоли MMC – см. инструкцию на стр. 82).	**Постоянная защита файлов**
• Параметры автоматического блокирования доступа с компьютеров (см. инструкцию на стр. 306); • исключение компьютеров из блокирования (Доверенные компьютеры) (см. инструкцию на стр. 307); • предотвращение вирусных эпидемий (см. инструкцию на стр. 308).	**Блокирование доступа с компьютеров**
• Разрешение или запрет выполнения подозрительных скриптов (подробнее о параметре читайте в п. 6.1 на стр. 67); • применение доверенной зоны (подробнее о доверенной зоне – Глава 8 на стр. 108).	**Проверка скриптов**
• Управление списком доверенных процессов (так же как в диалоговом окне **Параметры приложения**, см. п. 20.7.1 на стр. 322); • отключение постоянной защиты файлов, доступ к которым осуществляется в операциях резервного копирования (так же как в диалоговом окне **Параметры приложения**, см. п. 20.7.2 на стр. 324); • создание и применение исключений доверенной зоны (см. п. 20.7 на стр. 322).	**Доверенная зона**

Параметры	**Закладка**
Параметры безопасности в задачах проверки по требованию (единые для всей области защиты): вы можете выбрать предустановленный уровень безопасности (см. описание в п. 9.2.2.1 на стр. 131) или настроить параметры безопасности вручную (так же как в консоли MMC – см. инструкцию на стр. 136).	**Проверка по требованию**
Параметры задач обновления **Обновление баз приложения** и **Обновление модулей приложения**: • выбрать источник обновлений (подробнее о параметре читайте в п. A.5.1 на стр. 426); • настроить параметры соединения с источником обновлений и указать расположение защищаемого сервера для оптимизации обновлений (кнопка **Настройка LAN**) (так же как в консоли MMC, см. инструкцию на стр. 161); • настроить параметры задачи **Обновление модулей приложения** (кнопка **Настройка**) (так же как в консоли MMC, см. инструкцию на стр. 163).	**Обновление**
Параметры задачи **Копирование обновлений**: • выбрать источник обновлений (подробнее о параметре читайте в п. A.5.1 на стр. 426); • настроить параметры соединения с источником обновлений и указать расположение защищаемого сервера для оптимизации обновлений (кнопка **Настройка LAN**) (так же как в консоли MMC, см. инструкцию на стр. 161); • настроить параметры задачи **Копирование обновлений** (так же как в консоли MMC, см. инструкцию на стр. 165).	**Копирование обновлений**
Отключение действия расписания системных задач (см. п. 19.4 на стр. 294)	**Системные задачи**
Параметры карантина (так же как в диалоговом окне **Параметры приложения**, см. инструкцию на стр. 315)	**Карантин**

Параметры	Закладка
Параметры резервного хранилища (так же как в диалоговом окне **Параметры приложения**, см. инструкцию на стр. 318)	**Резервное хранилище**
Общие параметры Антивируса	**Производительность** и **Дополнительно**
Настройка уведомлений администратора и пользователей о событиях Антивируса	**Уведомления**
Настройка отчетов	**Отчеты**
Настройка уведомлений администратора и пользователей о событиях Антивируса	**События**

4. После того как вы настроите нужные параметры политики, нажмите на кнопку **ОК**, чтобы сохранить изменения.

19.4. Отключение / возобновление запуска по расписанию локальных системных задач

С помощью политик вы можете на всех серверах одной группы администрирования отключать запуск по расписанию следующих локальных системных задач:

- **Постоянная защита файлов**;
- **Проверка скриптов**;
- задач проверки по требованию **Проверка моего компьютера**, **Проверка объектов на карантине**, **Проверка при старте системы** и **Проверка целостности приложения**;
- задач обновления **Обновление баз приложения**, **Обновление модулей приложения и Копирование обновлений**.

Примечание

Если вы исключите защищаемый сервер из группы администрирования, расписание системных задач будет автоматически включено.

Чтобы отключить запуск по расписанию системной задачи Антивируса на серверах группы:

1. В дереве Консоли администрирования разверните узел **Группы**, разверните нужную группу и в ней выберите узел **Политики**.
2. В панели результатов откройте контекстное меню на названии политики, с помощью которой вы хотите отключить запуск по расписанию системных задач Антивируса на серверах группы, и выберите команду **Свойства**.
3. В диалоговом окне **Свойства: <Название политики>** откройте закладку **Системные задачи** (см. рис. 101).

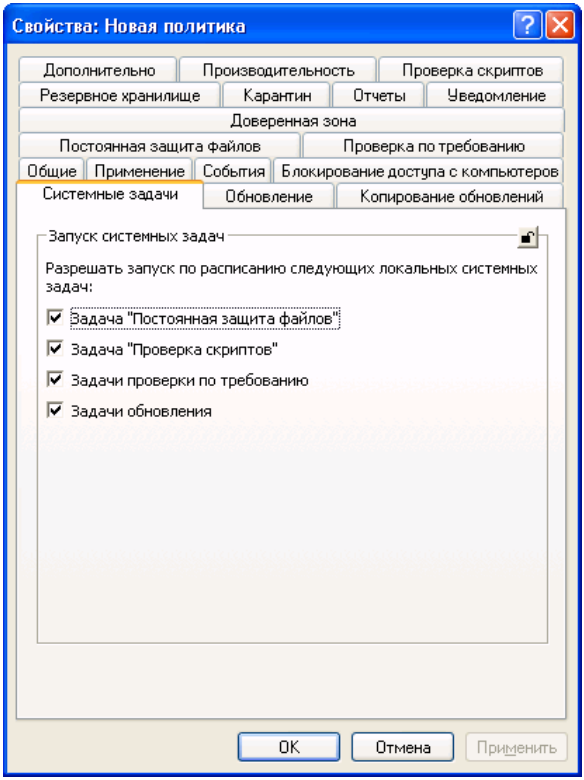

Рисунок 101. Диалоговое окно **Свойства: <Название политики>**, закладка **Системные задачи**

4. Снимите флажок рядом с именем системной задачи, запуск которой по расписанию вы хотите отключить.

Чтобы возобновить действие расписания системной задачи, установите флажок рядом с ее именем.

5. Нажмите на кнопку **ОК**.

Примечание

Если вы отключите запуск системных задач по расписанию, вы сможете запускать их вручную, как из консоли Антивируса в MMC, так и из Консоли администрирования Kaspersky Admnistration Kit.

ГЛАВА 20. НАСТРОЙКА АНТИВИРУСА В ДИАЛОГОВОМ ОКНЕ ПАРАМЕТРЫ ПРИЛОЖЕНИЯ

В этой главе содержится следующая информация:

- настройка параметров Антивируса (см. п. 20.2 на стр. 300);
- блокирование доступа с компьютеров (см. п. 20.3 на стр. 303);
- управление объектами на карантине и настройка параметров карантина (см. п. 20.4 на стр. 313);
- управление файлами в резервном хранилище и настройка параметров резервного хранилища (см. п. 20.5 на стр. 317);
- настройка уведомлений администратора и пользователей о событиях Антивируса (см. п. 20.6 на стр. 319);
- управление доверенной зоной (см. п. 20.7 на стр. 322).

О том, как открыть диалоговое окно **Параметры приложения**, см. п. 20.1 на стр. 297.

20.1. Диалоговое окно *Параметры приложения*

В диалоговом окне **Параметры приложения** вы можете выполнять операции по удаленному управлению Антивирусом и его настройке на выбранном защищаемом сервере.

*Чтобы открыть диалоговое окно **Параметры приложения**:*

1. В дереве Консоли администрирования разверните узел **Группы** и выберите группу, к которой принадлежит защищаемый сервер.

2. В панели результатов откройте контекстное меню на строке с информацией о защищаемом сервере и выберите команду **Свойства**.

3. В диалоговом окне **Свойства: <Имя компьютера>** на закладке **Приложения** выберите команду **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** в списке установленных приложений (см. рис. 102) и нажмите на кнопку **Свойства**.

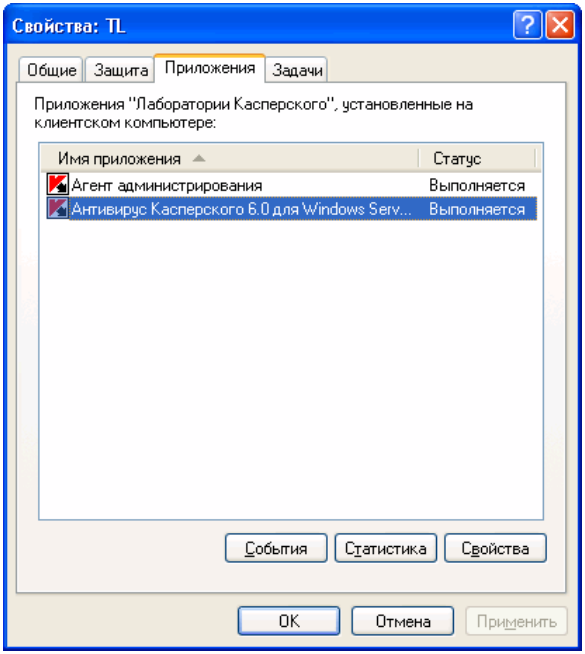

Рисунок 102. Список антивирусных приложений в диалоговом окне **Свойства: <Имя компьютера>**

Откроется диалоговое окно **Параметры приложения** (см. рис. 103).

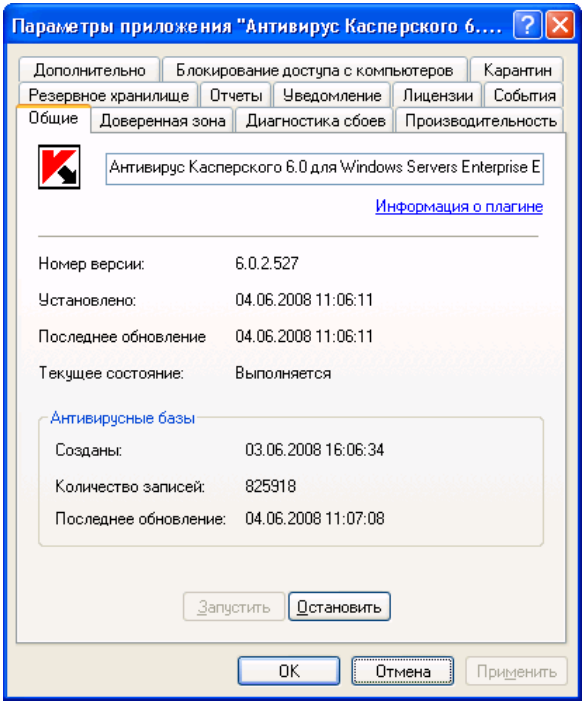

Рисунок 103. Диалоговое окно **Параметры приложения**, закладка **Общие**

Примечание

Во время действия политики Kaspersky Administration Kit значения параметров, помеченные в политике значком 🔒, не доступны для редактирования в диалоговом окне **Свойства приложения** Консоли администрирования.

20.2. Настройка общих параметров Антивируса

Чтобы настроить общие параметры Антивируса:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297).

   На следующих закладках измените значения общих параметров Антивируса согласно вашим требованиям.

   - На закладке **Производительность** (см. рис. 104):
     - установите максимальное количество рабочих процессов, которые Антивирус может запустить (см. п. A.1.1 на стр. 373);
     - установите фиксированное количество процессов для задач постоянной защиты (см. п. A.1.2 на стр. 374);
     - установите максимальное количество процессов для фоновых задач проверки по требованию (см. п. A.1.3 на стр. 376);
     - задайте количество попыток восстановления задач после аварийного их завершения (см. п. A.1.4 на стр. 377).

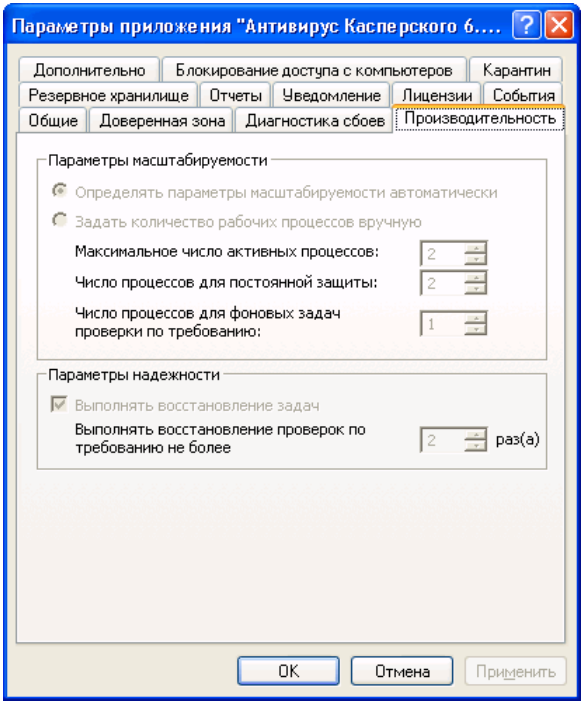

Рисунок 104. Диалоговое окно **Параметры приложения**, закладка **Производительность**

- На закладке **Дополнительно** (см. рис. 105):
  - укажите, отображать ли значок Антивируса в области уведомлений панели задач сервера, каждый раз, когда Антивирус будет автоматически запущен после перезагрузки сервера (подробнее о значке Антивируса читайте в п. 2.4 на стр. 37).
  - укажите, сколько дней будут храниться сводные и подробные отчеты о выполнении задач, которые отображаются в узле **Отчеты** в консоли Антивируса в ММС (см. п. A.1.5 на стр. 378);
  - укажите, сколько дней будет храниться информация, которая отображается в консоли Антивируса в ММС в узле **Журнал системного аудита** (см. п. A.1.6 на стр. 379);
  - укажите действия Антивируса при работе сервера от источника бесперебойного питания (см. п. A.1.7 на стр. 379);

- установите пороговое количество дней, после которого возникают события *Базы устарели*, *Базы сильно устарели* и *Полная проверка компьютера выполнялась давно* (см. п. A.1.8 на стр. 380).

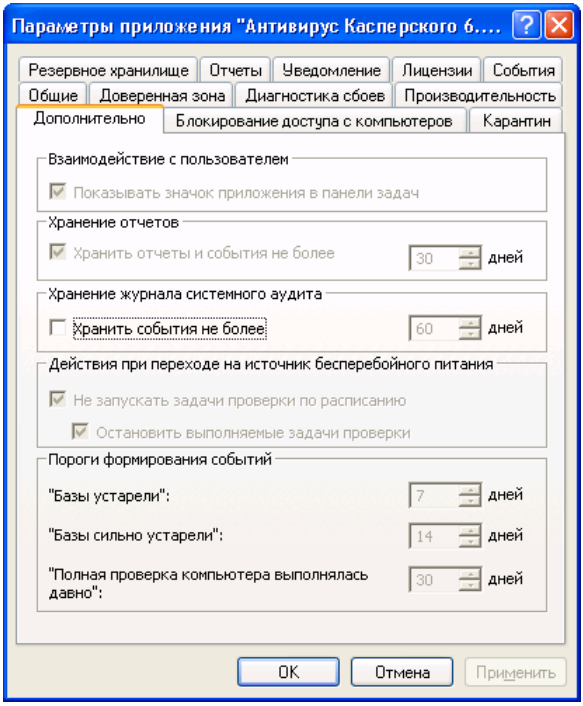

Рисунок 105. Диалоговое окно **Параметры приложения**, закладка **Дополнительно**

- На закладке **Диагностика сбоев** (см. рис. 106):
  - включите или выключите создание журнала трассировки; если создание журнала трассировки включено, настройте параметры журнала (см. п. A.1.9 на стр. 381);
  - включите или выключите создание файлов дампов памяти процессов Антивируса (см. п. A.1.10 на стр. 388).

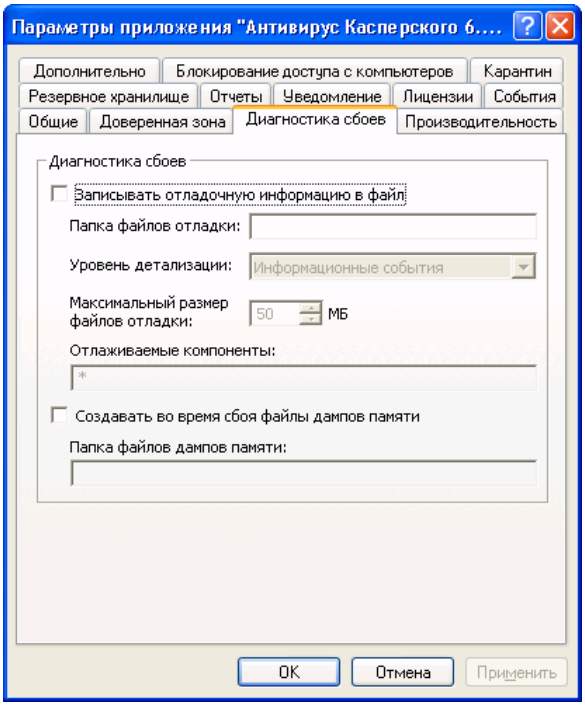

Рисунок 106. Диалоговое окно **Параметры приложения**, закладка **Диагностика сбоев**

2. После того как вы измените значения нужных параметров Антивируса, нажмите на кнопку **ОК**.

20.3. Блокирование доступа с компьютеров

В диалоговом окне **Параметры приложения** вы можете управлять блокированием доступа с компьютеров и предотвращением вирусных эпидемий (подробнее читайте в п. 7.1 на стр. 96).

Вы можете выполнять следующие операции:

- включать или отключать автоматическое блокирование доступа с компьтеров (см. п. 20.3.1 на стр. 304);

- настраивать параметры автоматического блокирования доступа с компьютеров (см. п. 20.3.2 на стр. 305);
- добавлять компьютеры в список исключенных из блокирования (см. п. 20.3.3 на стр. 307);
- включать автоматическое повышение уровня безопасности, если количество заблокированных компьютеров достигнет порогового (функция *Предотвращение вирусных эпидемий*) (см. п. 20.3.4 на стр. 308);
- просматривать список блокирования доступа (см. п. 20.3.5 на стр. 310);
- блокировать доступ с компьютеров вручную (см. п. 20.3.6 на стр. 311);
- открыть доступ с компьютеров (см. п. 20.3.7 на стр. 313).

20.3.1. Включение или отключение автоматического блокирования доступа с компьютеров

Подробнее о работе функции автоматического блокирования доступа с компьютеров читайте в А.4.1 на стр. 419.

Примечание

Если вы включите функцию автоматического блокирования доступа с компьютеров, она будет выполняться только тогда, когда выполняется задача **Постоянная защита файлов**.

Чтобы включить или выключить функцию блокирования доступа с компьютеров:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297).
2. На закладке **Блокирование доступа с компьютеров** (см. рис. 107) выполнить одно из следующих действий:
   - чтобы включить функцию автоматического блокирования доступа с компьютеров, установите флажок **Включить блокирование доступа с компьютеров к серверу**;

- чтобы отключить функцию автоматического блокирования доступа с компьютеров, снимите флажок **Включить блокирование доступа с компьютеров к серверу**.

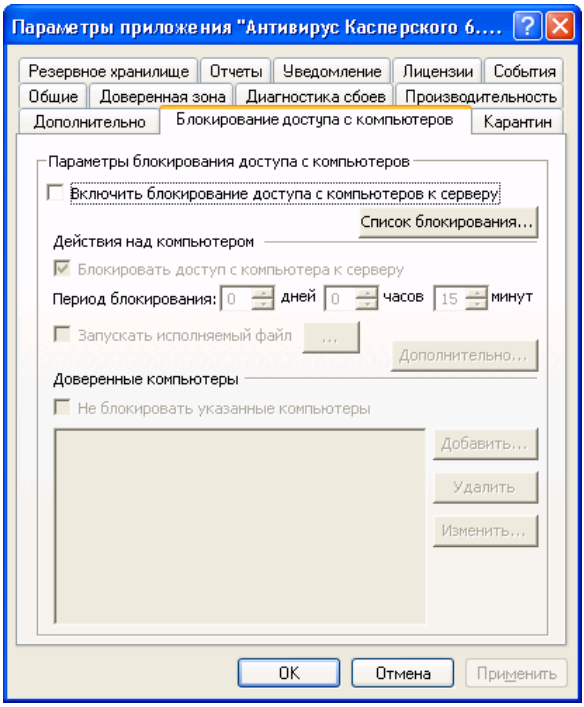

Рисунок 107. Диалоговое окно **Параметры приложения**, закладка **Блокирование доступа с компьютеров**

20.3.2. Настройка параметров автоматического блокирования доступа с компьютеров

Чтобы настроить параметры автоматического блокирования доступа с компьютеров:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297).

2. На закладке **Блокирование доступа с компьютеров** убедитесь, что флажок **Включить блокирование доступа с компьютеров к серверу** установлен (см. п. A.4.1 на стр. 419).

3. В группе параметров **Действия над компьютером** выберите действия, которые Антивирус выполнит при попытке записи с компьютера на сервер зараженного или подозрительного объекта (см. п. A.4.2 на стр. 420).

   - Если вы выбрали **Блокировать доступ с компьютера к серверу**, то задайте промежуток времени, на который вы хотите заблокировать доступ к серверу с указанных компьютеров, в днях, часах или минутах.
   - Если вы выбрали **Запустить исполняемый файл**, то нажмите на кнопку списка ... и в диалоговом окне **Исполняемый файл** (см. рис. 108) укажите исполняемый файл (имя и полный путь к нему), а также учетную запись, с правами которой исполняемый файл будет выполнен.

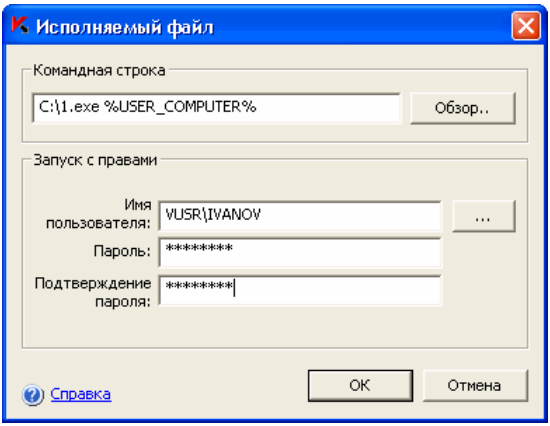

Рисунок 108. Диалоговое окно **Исполняемый файл**

4. Нажмите на кнопку **ОК** в диалоговом окне **Параметры приложения**.

20.3.3. Исключение компьютеров из блокирования (Доверенные компьютеры)

Чтобы добавить компьютер в список исключенных из блокирования (см. п. A.4.3 на стр. 421):

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297).
2. На закладке **Блокирование доступа с компьютеров** убедитесь, что флажок **Включить блокирование доступа с компьютеров к серверу** установлен (см. п. A.4.1 на стр. 419).
3. В группе параметров **Доверенные компьютеры** установите флажок **Не блокировать доступ с компьютеров** и выполните следующие действия:

   а) Нажмите на кнопку **Добавить** и укажите компьютер в диалоговом окне **Добавление компьютера** (см. рис. 109). Выполните одно из следующих действий:

   - выберите **Использовать сетевое имя компьютера** и укажите NetBIOS-имя компьютера;
   - укажите единственный IP-адрес: выберите **Использовать сетевой IP-адрес компьютера** и введите IP-адрес компьютера;
   - укажите диапазон IP-адресов: выберите **Использовать диапазон IP-адресов**. Введите первый IP-адрес диапазона в поле **Начальный IP-адрес**, а последний IP-адрес в поле **Конечный IP-адрес**. Все компьютеры, IP-адреса которых входят в указанный диапазон, будут считаться доверенными.

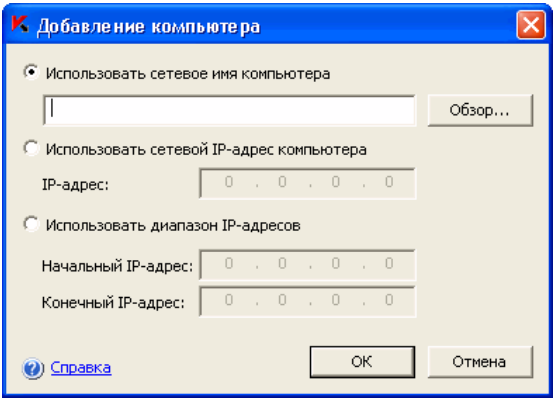

Рисунок 109. Диалоговое окно **Добавление компьютера**

б) Нажмите на кнопку **ОК**.

4. Нажмите на кнопку **ОК** в диалоговом окне **Параметры приложения**.

20.3.4. Предотвращение вирусных эпидемий

Вы можете использовать функцию *Предотвращение вирусных эпидемий* – когда функция включена, Антивирус автоматически повышает уровень безопасности, как только количество заблокированных компьютеров достигает порогового.

Описание функции *Предотвращение вирусных эпидемий* приводится в п. A.4.4 на стр. 422.

Чтобы включить / выключить функцию Предотвращение вирусных эпидемий:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297).
2. На закладке **Блокирование доступа с компьютеров** убедитесь, что флажок **Включить блокирование доступа с компьютеров к серверу** установлен.
3. Нажмите на кнопку **Дополнительно**.
4. В диалоговом окне **Дополнительно** (см. рис. 110) выполните одно из следующих действий.

- Чтобы включить функцию *Предотвращение вирусных эпидемий*:

  а) установите флажок **Повышать уровень безопасности, если число компьютеров более**;

  б) укажите количество заблокированных компьютеров в списке блокирования, по достижению которого Антивирус повысит уровень безопасности;

  в) включите или выключите восстановление уровня безопасности, когда количество компьютеров, доступ с которых к серверу заблокирован, снизится до указанного. Укажите количество компьютеров в поле **Восстанавливать уровень безопасности, если число компьютеров менее**.

- Чтобы выключить функцию *Предотвращение вирусных эпидемий*, снимите флажок **Повышать уровень безопасности, если число компьютеров более**.

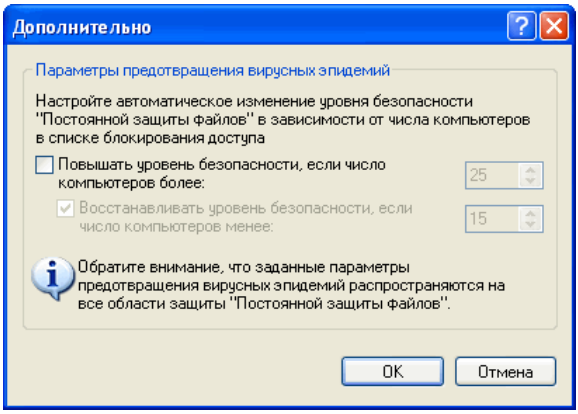

Рисунок 110. Диалоговое окно **Дополнительно**

5. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **ОК** в диалоговом окне **Параметры приложения**.

20.3.5. Просмотр списка блокирования доступа к серверу

Внимание!

Компьютерам в списке блокирования доступа к серверу запрещен доступ к защищаемому серверу только тогда, когда выполняется задача **Постоянная защита файлов** и включено автоматическое блокирование доступа с компьютеров.

Чтобы просмотреть список компьютеров, с которых в текущий момент заблокирован доступ к защищаемому серверу:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297).
2. На закладке **Блокирование доступа с компьютеров** нажмите на кнопку **Список блокирования** (см. рис. 111).

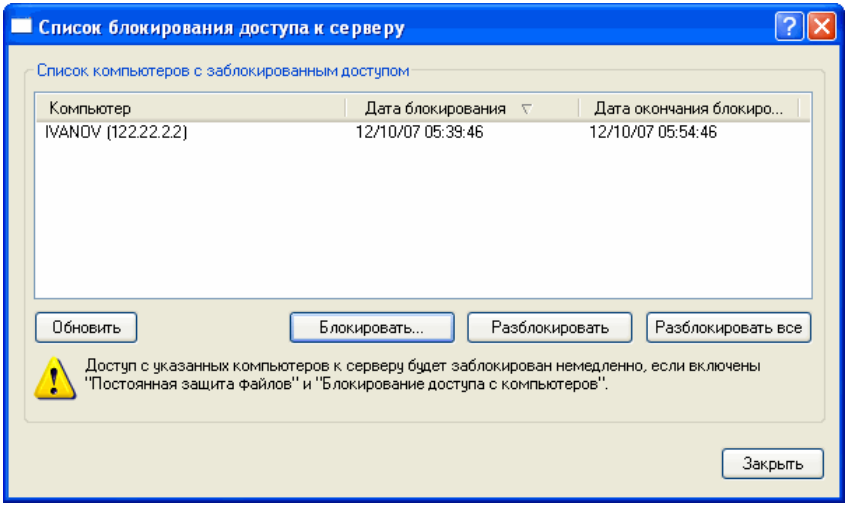

Рисунок 111. Диалоговое окно **Список блокирования доступа к серверу**

В диалоговом окне **Список блокирования доступа к серверу** отображается следующая информация о компьютерах, которым в текущий момент запрещен доступ к защищаемому серверу:

Поле	Описание
Компьютер	Информация о компьютере в списке блокирования, полученная Антивирусом (сетевое имя, IP-адрес)
Дата блокирования	Дата и время, когда доступ с компьютера был заблокирован; отображается в формате, заданном региональными настройками Microsoft Windows компьютера, на котором установлена Консоль администрирования.
Дата окончания блокирования	Дата и время, когда компьютер будет разблокирован; отображается в формате, заданном региональными настройками Windows компьютера, на котором установлена Консоль администрирования.

20.3.6. Блокирование доступа с компьютеров вручную

Если у вас есть информация о том, что какой-либо компьютер в локальной сети заражен, вы можете вручную временно заблокировать доступ с него к защищаемому серверу.

Внимание!

Компьютерам в списке блокирования доступа к серверу запрещен доступ к защищаемому серверу только тогда, когда выполняется задача **Постоянная защита файлов** и включено автоматическое блокирование доступа с компьютеров.

Чтобы заблокировать доступ к серверу с компьютера:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297).
2. На закладке **Блокирование доступа с компьютеров** нажмите на кнопку **Список блокирования**.
3. В диалоговом окне **Список блокирования** нажмите на кнопку **Блокировать**.

4. В диалоговом окне **Блокирование доступа с компьютера** (см. рис. 112) укажите сетевое имя компьютера, доступ с которого вы хотите заблокировать.

> **Примечание**
>
> В поле **Имя компьютера** указывайте только сетевые NetBIOS-имена компьютеров; не указывайте DNS-адреса.

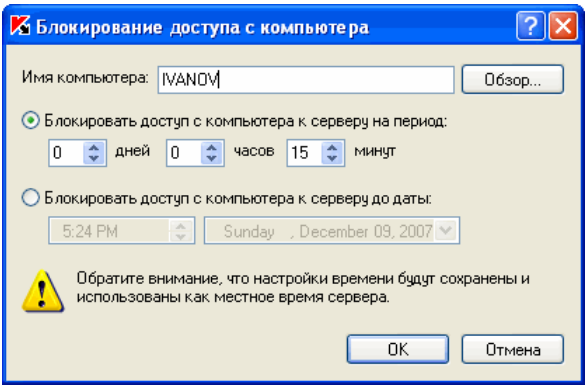

Рисунок 112. Диалоговое окно **Блокирование доступа с компьютера**

> **Примечание**
>
> Рекомендуется указать сетевое имя компьютера, который вы хотите добавить в список блокирования.

5. Затем выполните одно из следующих действий:

   - выберите **Заблокировать доступ с компьютера к серверу на период** и укажите промежуток времени, в течение которого доступ с компьютера к серверу будет запрещен;
   - выберите **Заблокировать доступ с компьютера к серверу до даты** и укажите дату и время, когда компьютер будет разблокирован.

   > **Примечание**
   >
   > Указывайте дату и время относительно текущей даты и текущего времени по часам защищаемого сервера.

6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **ОК** в диалоговом окне **Параметры приложения**.

20.3.7. Разблокирование доступа с компьютеров

Чтобы разблокировать доступ с компьютера:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297).
2. На закладке **Блокирование доступа с компьютеров** нажмите на кнопку **Список блокирования**.
3. В диалоговом окне **Список блокирования** в списке заблокированных компьютеров выберите компьютер, который вы хотите разблокировать, и нажмите на кнопку **Разблокировать компьютер**.

   Чтобы разблокировать все заблокированные компьютеры, нажмите на кнопку **Разблокировать все**.
4. Нажмите на кнопку **ОК**.
5. Нажмите на кнопку **ОК** в диалоговом окне **Параметры приложения**.

20.4. Управление объектами на карантине и настройка параметров карантина

20.4.1. Функции карантина и средства их настройки

В следующей таблице перечислены функции карантина и средства администрирования, с помощью которых вы можете управлять этими функциями.

Таблица 27. Функции карантина и средства их настройки

Функция карантина	Консоль администрирования Kaspersky Administration Kit	Консоль Антивируса в ММС
Просмотр, сортировка, удаление объектов	Да (см. документ *Kaspersky Administration Kit. Руководство администратора*)	Да
Фильтрация объектов	Нет	Да
Отправка подозрительных объектов из карантина на исследование в «Лабораторию Касперского»	Нет	Да
Помещение объектов на карантин вручную	Нет	Да
Восстановление объектов из карантина	Да (только в исходное местоположение)	Да
Проверка объектов на карантине	Да Запустите задачу **Проверка объектов на карантине**.	Да
Настройка параметров карантина	Да См. п. 20.4.2 на стр. 315.	Да
Просмотр статистики карантина	Да См. «Просмотр статистики Антивируса», п. 18.3 на стр. 278.	Да

20.4.2. Настройка параметров карантина

В диалоговом окне **Параметры приложения** выбранного защищаемого сервера вы можете настраивать параметры карантина.

Информация об изолировании подозрительных объектов приводится в п. 11.1 на стр. 169.

Чтобы настроить параметры карантина:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297).
2. На закладке **Карантин** (см. рис. 113), если требуется, измените параметры карантина:
   - чтобы указать другую папку-местоположение карантина, в поле **Папка карантина** выберите нужную папку на диске или введите полный путь к ней (см. п. А.6.1 на стр. 438);
   - чтобы указать максимальный размер карантина, установите флажок **Максимальный размер карантина** и укажите нужное значение параметра в мегабайтах (см. п. А.6.2 на стр. 439);
   - чтобы указать порог свободного пространства в карантине, установите флажок **Максимальный размер карантина**, установите флажок **Порог свободного места** и укажите нужное значение параметра в мегабайтах (см. п. А.6.3 на стр. 440);
   - чтобы указать другую папку для восстановленных объектов, в группе параметров **Параметры восстановления объектов** выберите нужную папку на диске или введите полный путь к ней (см. п. А.6.4 на стр. 441).

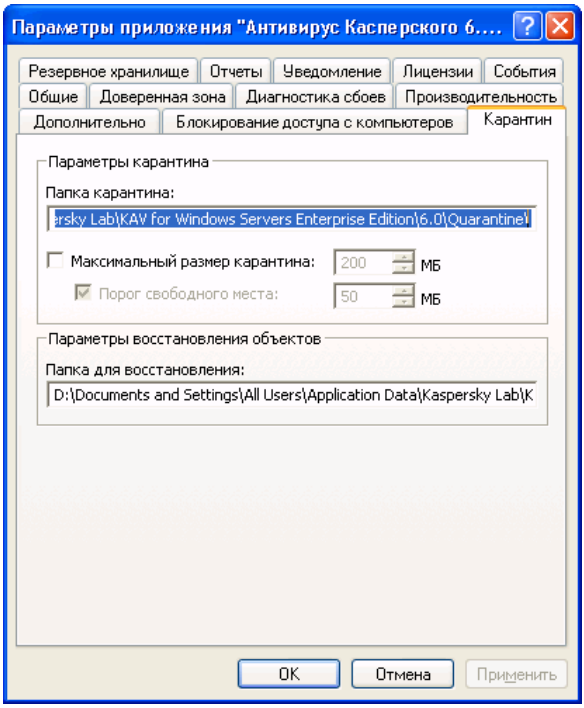

Рисунок 113. Диалоговое окно **Параметры приложения**, закладка **Карантин**

3. Нажмите на кнопку **ОК**.

20.5. Управление файлами в резервном хранилище и настройка параметров резервного хранилища

20.5.1. Функции резервного хранилища и средства их настройки

В следующей таблице перечислены функции резервного хранилища и средства администрирования, с помощью которых вы можете управлять этими функциями.

Таблица 28. Функции резервного хранилища

Функция резервного хранилища	**Консоль администрирования Kaspersky Administration Kit**	**Консоль Антивируса в MMC**
Просмотр, сортировка, удаление файлов	Да	Да
Фильтрация файлов	Нет	Да
Восстановление файлов из резервного хранилища	Да (только в исходное местоположение)	Да
Настройка параметров резервного хранилища	Да См. п. 20.5.2 на стр. 318.	Да
Просмотр статистики резервного хранилища	Да См. «Просмотр статистики Антивируса», п. 18.3 на стр. 278.	Да

20.5.2. Настройка параметров резервного хранилища

В диалоговом окне **Параметры приложения** выбранного защищаемого сервера вы можете настраивать параметры резервного хранилища.

О резервном копировании объектов перед их лечением или удалением читайте в п. 12.1 на стр. 189.

Чтобы настроить параметры резервного хранилища:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297), откройте закладку **Резервное хранилище**.
2. На закладке **Резервное хранилище** настройте нужные параметры резервного хранилища (см. рис. 114):
   - чтобы указать другую папку-местоположение резервного хранилища, в поле **Папка резервного хранилища** выберите нужную папку на диске или введите полный путь к ней (см. п. A.7.1 на стр. 442);
   - чтобы изменить максимальный размер резервного хранилища, установите флажок **Максимальный размер хранилища** и укажите нужное значение параметра в мегабайтах (см. п. A.7.2 на стр. 444);
   - чтобы изменить порог свободного пространства в резервном хранилище, установите флажок **Максимальный размер хранилища**, убедитесь, что установлен флажок **Порог свободного места** и укажите нужное значение параметра в мегабайтах (см. п. A.7.3 на стр. 445);
   - чтобы указать другую папку для восстановленных объектов, в группе параметров **Параметры восстановления объектов** выберите нужную папку на диске или введите полный путь к ней (см. п. A.7.4 на стр. 446).

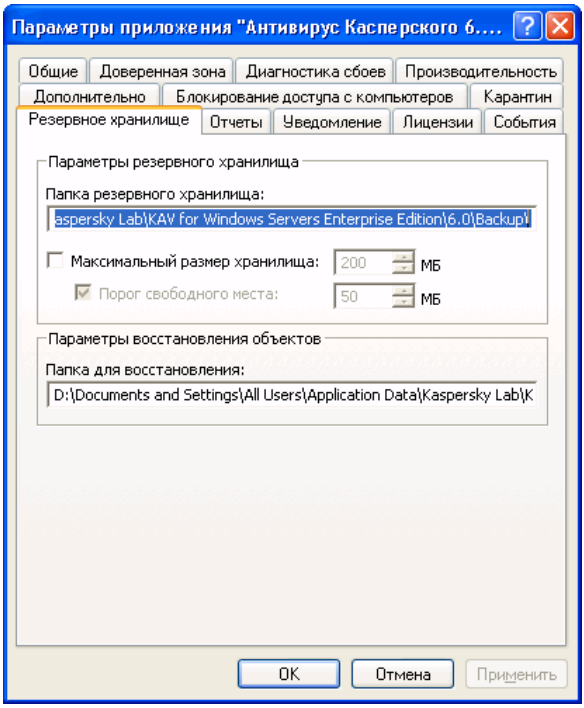

Рисунок 114. Диалоговое окно **Параметры приложения**, закладка **Резервное хранилище**

3. Нажмите на кнопку **ОК**.

20.6. Настройка уведомлений

В этом разделе содержится следующая информация:

- общая информация о настройке уведомлении через Консоль администрирования (см. п. 20.6.1 на стр. 320);
- Настройка уведомлений администратора и пользователей на закладке *Уведомление* (см. п. 20.6.2 на стр. 321).

20.6.1. Общая информация

В Консоли администрирования Kaspersky Administration Kit вы можете настроить уведомление администратора и пользователей о событиях, связанных с работой Антивируса и состоянием антивирусной защиты защищаемого сервера:

- администратор может получать информацию о событиях выбранных типов;
- пользователи локальной сети, которые обращаются к защищаемому серверу, могут получать информацию о событиях типов *Обнаружена угроза* и *Компьютер добавлен в список блокирования*; терминальные пользователи сервера могут получать информацию о событиях *Обнаружена угроза*.

Вы можете настроить уведомления о событиях Антивируса как для одного сервера в окне **Свойства приложения** выбранного сервера, так и для группы серверов в окне **Свойства политики** выбранной группы.

В этих диалоговых окнах вы можете настраивать уведомления на закладке **События** или на закладке **Уведомление**.

- на закладке **События** (стандартная закладка приложения Kaspersky Administration Kit) вы можете настраивать уведомления администратора о событиях выбранных типов. О том, какие способы уведомлений вы можете настроить и как это выполнить, читайте в документе *Kaspersky Administration Kit. Руководство администратора*;
- на закладке **Уведомление** вы можете настраивать уведомления как администратора, так и пользователей. Подробнее о способах уведомлений, которые вы можете настроить на закладке **Уведомление**, читайте в п. 15.1 на стр. 234. О том, как настраивать уведомления на закладке **Уведомление**, читайте в п. 20.6.2 на стр. 321.

Уведомления о событиях некоторых типов вы можете настраивать только на одной из закладок, о событиях других типов – на обеих.

Примечание

Если вы настроите уведомления о событиях одного типа одним способом сразу на двух закладках, и на закладке **События**, и на закладке **Уведомление**, то администратор будет получать уведомления об этих событиях этим способом дважды.

20.6.2. Настройка уведомлений администратора и пользователей на закладке *Уведомление*

Чтобы настроить уведомления:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297), откройте закладку **Уведомление**.
2. На закладке **Уведомление** (см. рис. 115) настройте уведомления о событиях нужных типов и нажмите на кнопку **ОК**.

Настройка уведомлений на закладке **Уведомление** аналогична настройке уведомлений в диалоговом окне **Уведомления** консоли Антивируса в ММС. Подробнее о том, как выполнить настройку, читайте в п. 15.2 на стр. 237.

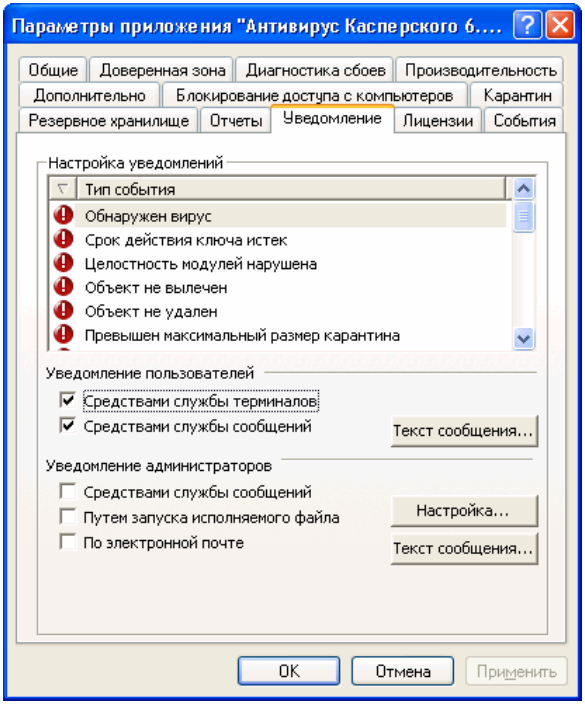

Рисунок 115. Диалоговое окно **Параметры приложения**, закладка **Уведомление**

20.7. Управление доверенной зоной

В этом разделе содержится следующая информация:

- добавление процессов в список доверенных (см. п. 20.7.1 на стр. 322);
- отключение постоянной защиты файлов на время резервного копирования (см. п. 20.7.2 на стр. 324);
- добавление исключений (см. п. 20.7.3 на стр. 325);
- применение доверенной зоны (см. п. 20.7.4 на стр. 329).

Подробнее о доверенной зоне Антивируса читайте в п. 8.1 на стр. 108.

20.7.1. Добавление процессов в список доверенных

В Консоли администрирования Kaspersky Administration Kit вы можете добавлять в доверенную зону исполняемые файлы процессов на диске защищаемого сервера; вы не можете добавлять процессы из списка активных процессов на сервере.

Подробнее о доверенной зоне Антивируса читайте в п. 8.1 на стр. 108.

Чтобы добавить процесс в список доверенных процессов Антивируса:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297), закладку **Доверенная зона** (см. рис. 116).
2. Включите функцию **Доверенные процессы**: установите флажок **Не проверять файловую активность указанных процессов**.

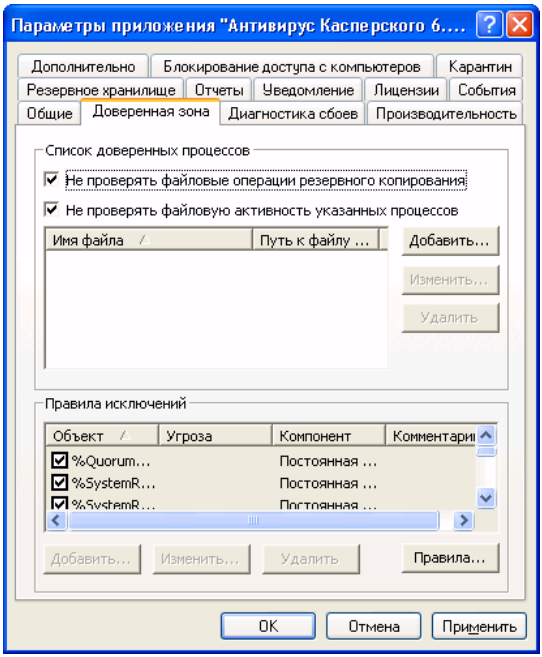

Рисунок 116. Диалоговое окно **Параметры приложения**, закладка **Доверенная зона**

3. Чтобы выбрать исполняемый файл процесса на диске защищаемого сервера, выполните следующее:

   а) На закладке **Доверенная зона** нажмите на кнопку **Добавить**;

   б) в диалоговом окне **Добавление доверенного процесса** нажмите на кнопку **Обзор** и выберите исполняемый файл процесса на локальном диске защищаемого сервера;

   В диалоговом окне **Добавление доверенного процесса** отобразится название файла и путь к нему.

   в) нажмите на кнопку **ОК**.

   Имя выбранного исполняемого файла процесса отобразится в списке доверенных процессов на закладке **Доверенная зона**.

4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

20.7.2. Отключение постоянной защиты файлов на время резервного копирования

На время резервного копирования файлов вы можете отключать постоянную защиту файлов, доступ к которым выполняется в операциях резервного копирования. Антивирус не проверяет файлы, которые приложение резервного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

Чтобы отключить постоянную защиту файлов на время резервного копирования:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297), закладку **Доверенная зона** (см. рис. 117).

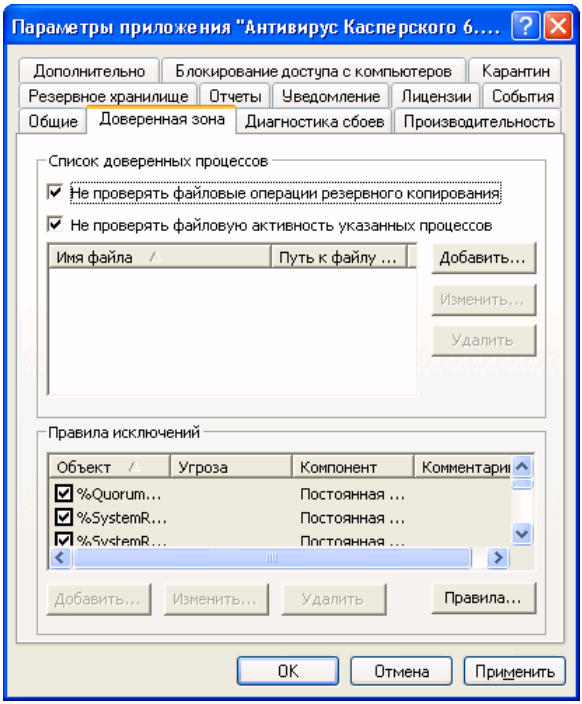

Рисунок 117. Диалоговое окно **Параметры приложения**, закладка **Доверенная зона**

2. Чтобы отключить постоянную защиту файлов, доступ к которым выполняется в задаче резервного копирования, установите флажок **Не проверять файловые операции резервного копирования**.
3. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
4. Примените исключения доверенной зоны в выбранных задачах и политиках (см. п. 20.7.4 на стр. 329).

20.7.3. Добавление исключений в доверенную зону

Вы можете добавлять в доверенную зону объекты для исключения из проверки. Подробнее о доверенной зоне читайте в п. 8.1 на стр. 108.

Чтобы добавить исключение:

1. Откройте диалоговое окно **Параметры приложения** (см. п. 20.1 на стр. 297), закладку **Доверенная зона** (см. рис. 116).
2. Нажмите на кнопку **Добавить** под заголовком **Правила исключений**.

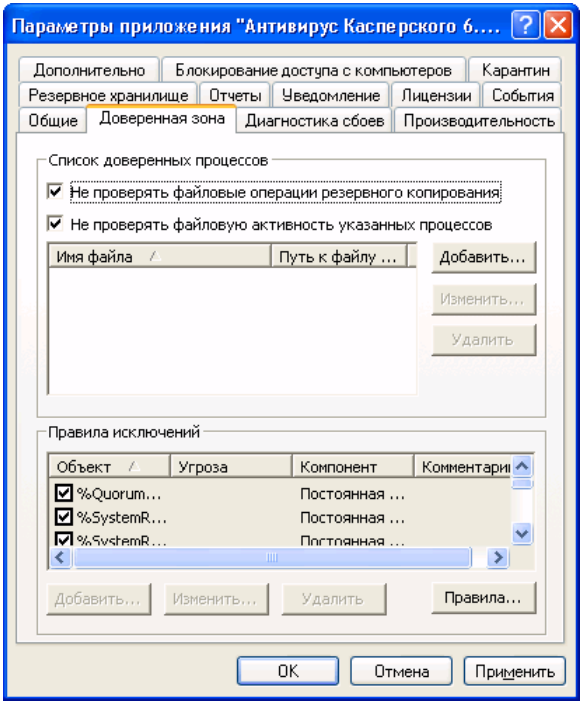

Рисунок 118. Диалоговое окно **Параметры приложения**, закладка **Доверенная зона**

Откроется диалоговое окно **Правило исключения**.

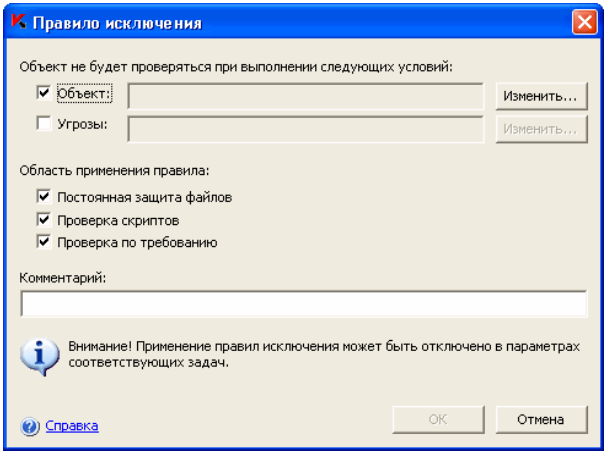

Рисунок 119. Диалоговое окно **Правило исключения**

3. Укажите правило, по которому Антивирус будет исключать объект.

> **Примечание**
>
> Чтобы исключить *указанные угрозы в указанных папках или файлах*, установите флажок **Объект** и флажок **Угрозы**.
>
> Чтобы исключить *все угрозы в указанных папках или файлах*, установите флажок **Объект**; снимите флажок **Угрозы**.
>
> Чтобы исключить *указанные угрозы во всей области проверки*, снимите флажок **Объект** и установите флажок **Угрозы**.

- *Если вы хотите указать местоположение объекта*, установите флажок **Объект**, нажмите на кнопку **Изменить** и в диалоговом окне **Выбор объекта** укажите объект, который будет исключен из проверки, а затем нажмите на кнопку **ОК**:
  - **Предопределенная область проверки**. Выберите в списке одну из предустановленных областей проверки.
  - **Диск или папка**. Укажите диск сервера или папку на сервере или в локальной сети.
  - **Файл**. Укажите файл на сервере или в локальной сети.
  - **Файл или URL-адрес скрипта**. Укажите скрипт на защищаемом сервере, в локальной сети или интернете..

Примечание

Вы можете задавать маски названий папок и файлов, используя символы ? и *.

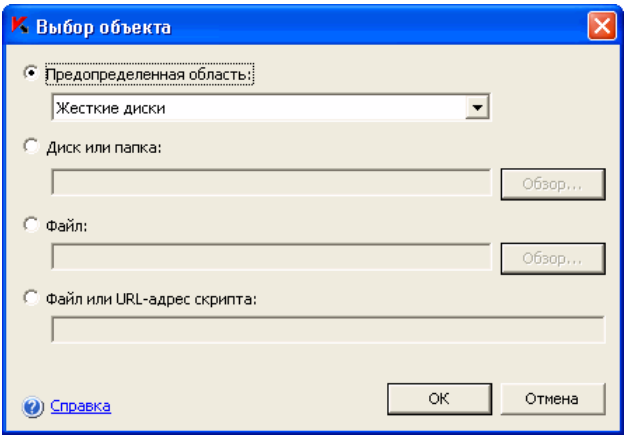

Рисунок 120. Диалоговое окно **Выбор объекта**

- *Если вы хотите указать название угрозы*, установите флажок **Угрозы**, нажмите на кнопку **Изменить** и в диалоговом окне **Список исключений угроз** добавьте названия угроз (подробнее о параметре читайте в п. A.3.9 на стр. 412).

4. Установите флажки рядом с названиями функциональных компонентов, в задачах которых правило исключения будет применяться.
5. Нажмите **ОК**.

- Чтобы отредактировать правило, на закладке **Доверенная зона** выберите правило, которое вы отредактировать, нажмите на кнопку **Изменить** и выполните изменение в диалоговом окне **Правило исключения**.
- Чтобы удалить правило, на закладке **Доверенная зона** выберите правило, которое вы удалить, нажмите на кнопку **Удалить** и подтвердите операцию.

6. Нажмите **ОК** в диалоговом окне **Параметры приложения**.
7. Если требуется, примените исключения доверенной зоны в выбранных задачах и политиках (см. п. 20.7.4 на стр. 329).

20.7.4. Применение доверенной зоны

Вы можете включать или выключать применение доверенной зоны в существующих политиках, а также в задачах (при создании задачи или в диалоговом окне **Свойства задачи**).

По умолчанию доверенная зона применяется во вновь созданных политиках и задачах.

Чтобы применить доверенную зону в политике:

1. В дереве Консоли администрирования разверните узел **Группы**, разверните группу администрирования, параметры политики которой вы хотите настроить, затем разверните вложенный узел **Политики**.
2. В панели результатов откройте контекстное меню на политике, параметры которой вы хотите настроить, и выберите команду **Свойства**.
3. В диалоговом окне **Свойства политики** выполните следующие действия:
   - чтобы применить исключения: *доверенные процессы*, убедитесь, что установлен флажок **Не проверять файловую активность указанных процессов** и установите замок в группе параметров **Список доверенных процессов**.
   - чтобы применить исключения: *операции резервного копирования*, убедитесь, что установлен флажок **Не проверять файловые операции резервного копирования** и установите замок в группе параметров **Список доверенных процессов**.
   - чтобы применить *исключения, указанные пользователем*, установите замок в группе параметров **Исключения**.
4. Нажмите на кнопку **ОК**.

Чтобы применить доверенную зону в существующей задаче:

1. В дереве Консоли администрирования разверните узел **Группы** и выберите группу, к которой принадлежит защищаемый сервер.
2. В панели результатов откройте контекстное меню на строке с информацией о защищаемом сервере и выберите команду **Свойства**.
3. В диалоговом окне **Свойства компьютера** на закладке **Задачи** откройте контекстное меню на задаче, которую вы хотите настроить, и выберите команду **Свойства**.

4. В диалоговом окне **Свойства задачи** на закладке **Настройка** нажмите на кнопку **Дополнительно** и в диалоговом окне **Дополнительно** установите значок **Применять доверенную зону**.

   Вы также можете применить доверенную зону при создании задачи.

ГЛАВА 21. СОЗДАНИЕ И НАСТРОЙКА ЗАДАЧ

В этой главе содержится следующая информация:

- о задачах, которые вы можете создавать в Консоли администрирования (см. п. 21.1 на стр. 331);
- создание задач (см. п. 21.2 на стр. 332);
- настройка задач (см. п. 21.3 на стр. 342).

21.1. О создании задач

Вы можете создавать локальные пользовательские, групповые и глобальные задачи следующих типов:

- проверка по требованию;
- задачи обновления;
- откат обновления баз;
- установка ключа.

Вы создаете локальные задачи для выбранного защищаемого сервера в диалоговом окне **Параметры** приложения на закладке **Задачи**, групповые задачи – в узле **Групповые задачи** выбранной группы, глобальные задачи – в узле **Глобальные задачи**.

Примечание

С помощью политик вы можете отключать действие расписания локальных системных задач на всех защищаемых серверах, принадлежащих к одной группе администрирования.

Общая информация о задачах в Kaspersky Administration Kit приводится в документе *Kaspersky Administration Kit. Руководство администратора*.

21.2. Создание задачи

Чтобы создать новую задачу в Консоли администрирования:

1. Запустите мастер создания задач нужной категории:

   - *для создания локальной задачи*:

     а) в дереве Консоли администрирования разверните узел **Группы** и выберите группу, которой принадлежит защищаемый сервер;

     б) в панели результатов откройте контекстное меню на строке с информацией о защищаемом сервере и выберите команду **Свойства**;

     в) на закладке **Задачи** нажмите на кнопку **Добавить**,

   - *для создания групповой задачи*:

     а) в дереве Консоли администрирования выберите группу, для которой вы хотите создать групповую задачу;

     б) откройте контекстное меню на вложенной папке **Групповые задачи** и выберите команду **Создать** → **Задачу**;

   - *для создания глобальной задачи* в дереве Консоли администрирования откройте контекстное меню на узле **Глобальные задачи** и выберите команду **Создать** → **Задачу**.

   Откроется окно приветствия мастера создания задач.

2. В окне **Имя задачи** мастера создания задач введите имя задачи (не более 100 символов, не может содержать символы **" * < > ? \ / | :)**. Рекомендуется включить в имя задачи ее тип (например, «Проверка по требованию папок общего доступа»).

3. В окне **Приложения**, под заголовком **Приложение**, выберите команду **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition**, под заголовком **Тип задачи** выберите тип создаваемой задачи.

4. В зависимости от типа создаваемой задачи выполните одно из следующих действий:

   - *Если вы создаете задачу проверки по требованию*:

     а) В окне **Область проверки** сформируйте область проверки.

По умолчанию область проверки включает предопределенную область **Мой компьютер** (см. рис. 121).

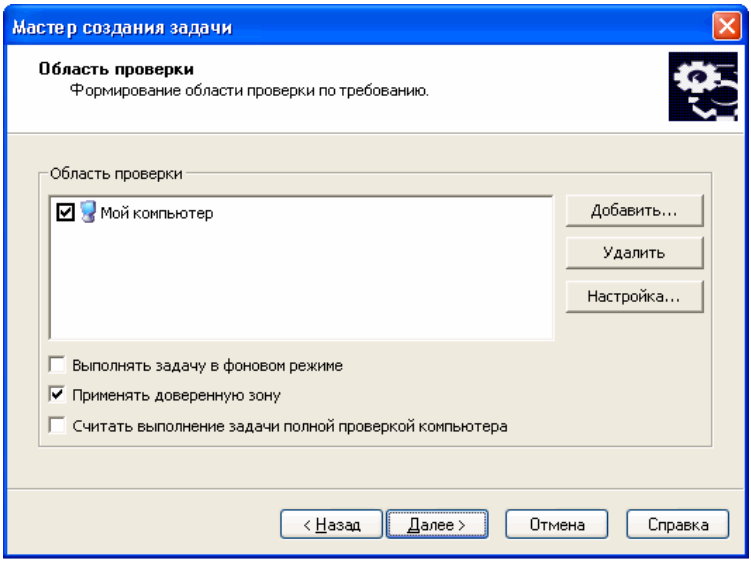

Рисунок 121. Окно **Область проверки** мастера создания задач

Область **Мой компьютер** содержит вложенные предопределенные области проверки (эти области описаны в п. 9.2.1.2 на стр. 124).

Если по требованиям к безопасности нет необходимости проверять весь сервер, вы можете ограничить область проверки: включить в нее только отдельные предопределенные области и / или отдельные диски, папки или файлы.

- Чтобы включить в область проверки только отдельные области, диски, папки или файлы, в диалоговом окне **Настройка** удалите предопределенную область **Мой компьютер**, затем нажмите на кнопку **Добавить**, в диалоговом окне **Добавление в область проверки** укажите объекты, которые войдут в область проверки: выберите предопределенную область в списке **Предопределенная область проверки** (см. рис. 122), укажите диск сервера, папку или файл на сервере или другом компьютере в сети, а затем нажмите на кнопку **ОК**.

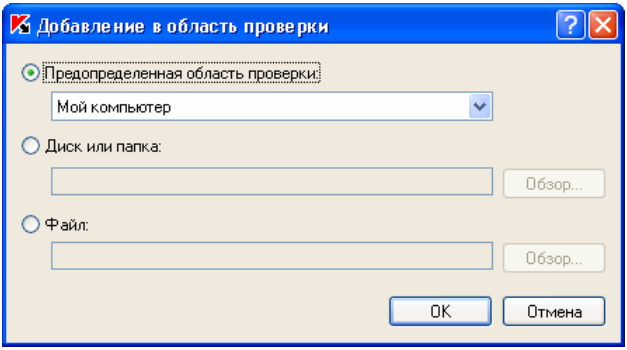

Рисунок 122. Диалоговое окно **Добавление в область проверки**

- Чтобы исключить из проверки вложенные папки или файлы, выберите добавленную папку (диск) в окне **Область проверки** мастера нажмите на кнопку **Настройка**, затем в окне **Настройка проверки по требованию** нажмите на кнопку **Настройка** и в диалоговом окне **Настройка области защиты** снимите флажок **Вложенные папки** (**Вложенные файлы**).
- Установите флажок **Применять доверенную зону**, если в задаче вы хотите исключить из области защиты объекты, описанные в доверенной зоне Антивируса (подробнее о доверенной зоне читайте в п. 8.1 на стр. 108; о том, как добавлять исключения в доверенную зону в приложении Kaspersky Administration Kit, читайте в п. 20.7 на стр. 322).

б) Если вы планируете использовать создаваемую задачу в качестве задачи полной проверки компьютера, установите флажок **Считать выполнение задачи полной проверкой сервера**. Приложение Kaspersky Administration Kit будет оценивать состояние безопасности сервера (серверов) по результатам выполнения задач со статусом «Задача полной проверки компьютера», а не по результатам выполнения системной задачи **Проверка Моего компьютера**. Подробнее о присвоении задаче проверки по требованию статуса «Задача полной проверки компьютера» читайте в п. 21.4 на стр. 344.

в) Чтобы присвоить рабочему процессу, в котором будет выполняться задача, базовый приоритет **Низкий** (**Low**), установите флажок **Выполнять в фоновом режиме**. По умолчанию рабочие процессы, в которых выполняются задачи Антивируса, имеют приоритет **Средний** (**Normal**). Пониже-

ние приоритета процесса увеличивает время выполнения задачи, но оно также может повлиять положительно на скорость выполнения процессов других активных приложений.

- *Если вы создаете одну из задач обновления, установите параметры задачи в соответствии с вашими требованиями*:

  а) выберите источник обновлений в окне **Источник обновлений** (см. п. A.5.1 на стр. 426);

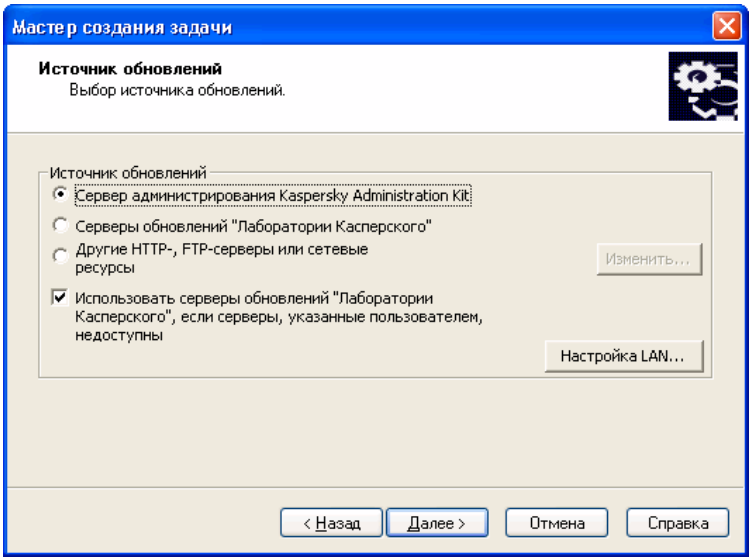

Рисунок 123. Окно **Источник обновлений**

  б) нажмите на кнопку **Настройка LAN**. Откроется диалоговое окно **Настройка соединения** (см. рис. 124);

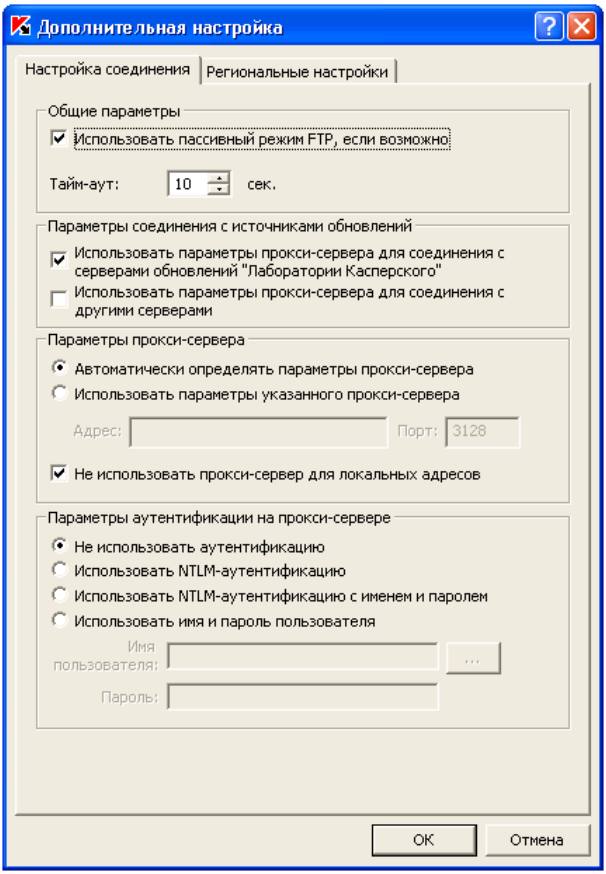

Рисунок 124. Диалоговое окно **Дополнительная настройка**, закладка **Настройка соединения**

в) на закладке **Настройка соединения** выполните следующие действия:

- укажите режим FTP-сервера для соединения с защищаемым сервером (см. п. A.5.2 на стр. 427);
- если требуется, измените время ожидания при соединении с источником обновлений (см. п. A.5.3 на стр. 428);
- настройте параметры доступа к прокси-серверу при соединении с источником обновлений (см. п. A.5.4 на стр. 429);

г) на закладке **Региональные настройки** укажите местоположение защищаемого сервера (серверов), чтобы оптимизировать получение обновлений (см. п. A.5.5 на стр. 432).

- *Если вы создаете задачу **Обновление модулей приложения***, в окне **Настройка обновления** (см. рис. 125) настройте нужные параметры обновления программных модулей:

а) выберите, загружать и устанавливать критические обновления программных модулей или только проверять их наличие (см. п. A.5.6.1 на стр. 433);

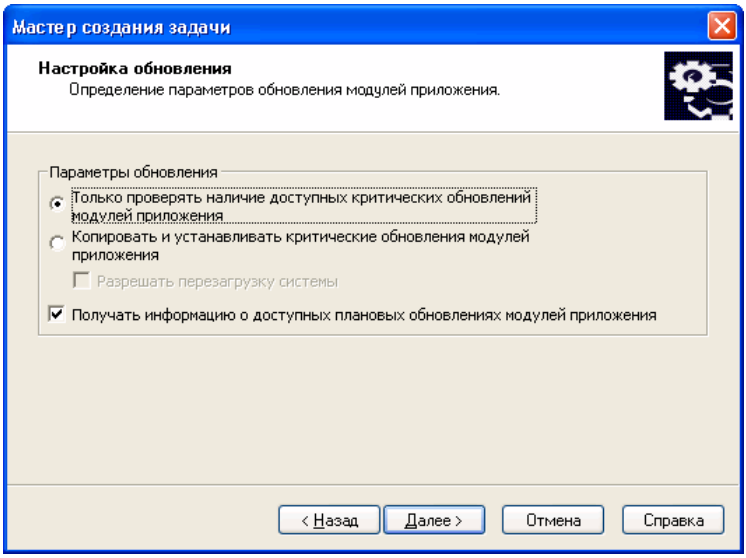

Рисунок 125. Окно **Настройка обновления** в задаче **Обновление модулей приложения**

б) если вы выбрали **Копировать и устанавливать критические обновления модулей приложения**: для применения установленных программных модулей может потребоваться перезагрузка сервера. Чтобы Антивирус автоматически запускал перезагрузку сервера после завершения задачи, установите флажок **Разрешать перезагрузку системы**. Чтобы отменить автоматическую перезагрузку после завершения задачи, снимите флажок **Разрешать перезагрузку системы**;

в) если вы хотите получать информацию о выходе плановых обновлений модулей Антивируса, установите флажок **По-**

лучать информацию о доступных плановых обновлениях.

«Лаборатория Касперского» не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете сами загружать их с вебсайта «Лаборатории Касперского». Вы можете настроить уведомление администратора о событии *Доступны плановые обновления модулей Антивируса*, в котором будет содержаться адрес страницы на нашем сайте, откуда вы сможете загружать плановые обновления (подробнее о настройке уведомлений читайте в п. 15.2 на стр. 237).

- *Если вы создаете задачу **Копирование обновлений***, в окне **Настройка копирования обновлений** укажите состав обновлений (см. п. A.5.7.1 на стр. 435) и папку для их сохранения (см. п. A.5.7.2 на стр. 437).

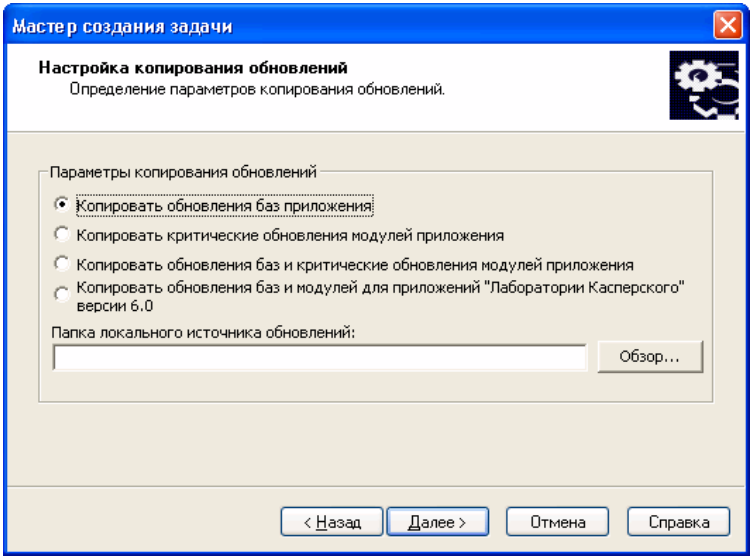

Рисунок 126. Окно **Настройка копирования обновлений**

- *Если вы создаете задачу **Установка ключа***, в окне **Установка ключа** (см. рис. 127) в поле **Ключ** укажите имя файла ключа с расширением .key и полный путь к нему.

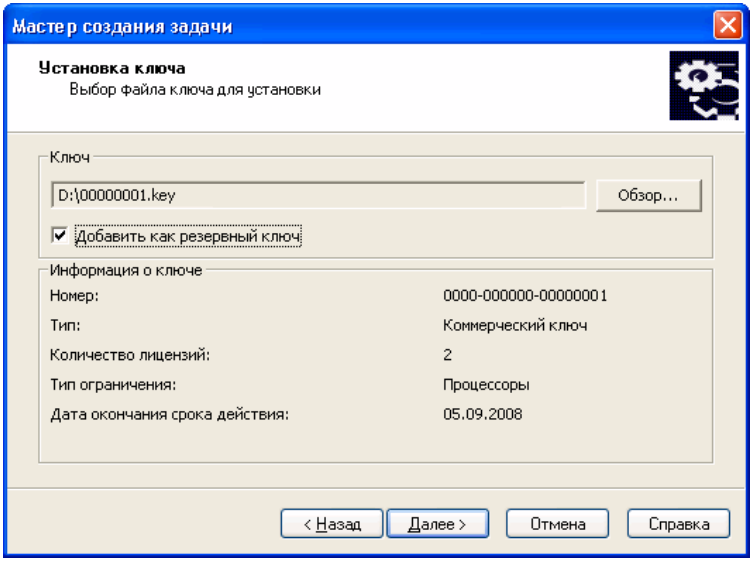

Рисунок 127. Окно **Установка ключа**

5. Настройте нужные параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задач **Установка ключа** и **Откат обновления баз**). В окне **Расписание** (см. рис. 128) выполните следующие действия:

   а) чтобы включить расписание, установите флажок **Запускать** задачу **по расписанию**;

   б) укажите частоту запуска задачи (см. п. A.2.1 на стр. 390): в списке **Частота запуска** выберите одно из следующих значений: **Ежечасно**, **Ежедневно**, **Еженедельно**, **При запуске Антивируса**, **При обновлении баз** (в задачах **Обновление баз приложения**, **Обновление модулей приложения** и **Копирование обновлений** вы также можете указать частоту запуска **После получения обновлений Сервером администрирования**):

      - если вы выбрали **Ежечасно**, укажите количество часов в поле **Каждые <количество> часов** в группе параметров **Параметры запуска задачи**;

      - если вы выбрали **Ежедневно**, укажите количество дней в поле **Каждые <количество> дней** в группе параметров **Параметры запуска задачи**;

- если вы выбрали **Еженедельно**, укажите количество недель в поле **Каждые <количество> недель** в группе параметров **Параметры запуска задачи**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача будет запускаться по понедельникам);

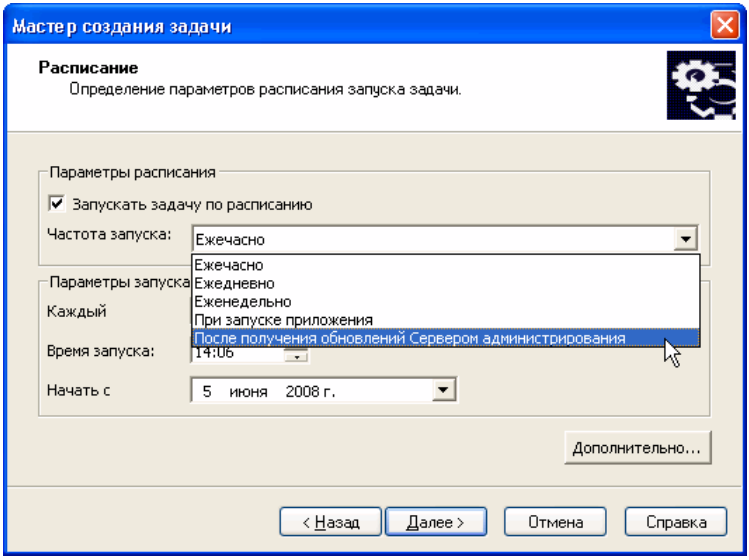

Рисунок 128. Пример окна **Расписание**, частота запуска **После получения обновлений Сервером администрирования**

в) в поле **Время запуска** укажите время первого запуска задачи; в поле **Начать с** укажите дату начала действия расписания (см. п. A.2.2 на стр. 392);

г) если требуется, задайте остальные параметры расписания: нажмите на кнопку **Дополнительно** и в диалоговом окне **Дополнительная настройка расписания** (см. рис. 129) выполните следующие действия:

- укажите максимальную продолжительность выполнения задачи: в группе **Параметры остановки задачи**, в поле **Длительность** введите нужное количество часов и минут (см. п. A.2.4 на стр. 394);

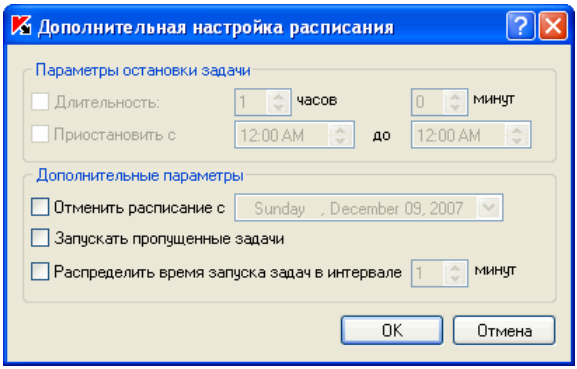

Рисунок 129. Диалоговое окно **Дополнительная настройка расписания**

- укажите промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено: в группе **Параметры остановки задачи** введите начальное и конечное значение промежутка в поле **Приостановить с … до** (см. п. A.2.5 на стр. 395);
- укажите дату, начиная с которой расписание перестанет действовать: установите флажок **Отменить расписание с** и с помощью диалогового окна **Календарь** выберите дату, начиная с которой расписание перестанет действовать (см. п. A.2.3 на стр. 393);
- включите запуск пропущенных задач: установите флажок **Запускать пропущенные задачи** (см. п. A.2.6 на стр. 396);
- включите использование параметра **Распределение времени запуска**: установите флажок **Распределить время запуска задач в интервале** и укажите значение параметра в минутах (см. п. A.2.7 на стр. 397);

д) нажмите на кнопку **ОК**.

6. Если создаваемая задача является глобальной, выберите компьютеры сети (группы), на которых она будет выполняться.
7. В окне **Завершение работы** мастера создания задач нажмите на кнопку **Готово**.

Созданная задача отобразится в диалоговом окне **Задачи**.

21.3. Настройка задачи

После того как вы создали задачу, вы можете выполнять следующие настройки:

- изменять параметры задачи;
- настраивать / изменять расписание задачи;
- указывать учетную запись, с правами которой задача будет выполняться;
- настраивать уведомление о результатах выполнения задачи.

Чтобы настроить задачу:

1. В дереве Консоли администрирования разверните узел **Группы** и выберите группу, к которой принадлежит защищаемый сервер.
2. В панели результатов откройте контекстное меню на строке с информацией о защищаемом сервере и выберите команду **Свойства**.
3. В диалоговом окне **Свойства компьютера** на закладке **Задачи** откройте контекстное меню на задаче, которую вы хотите настроить, и выберите команду **Свойства**.
4. Если требуется, измените параметры задачи:
   - в задаче **Постоянная защита файлов** на закладке **Настройка**:

     сформируйте область защиты (о предопределенных областях читайте в п. 6.2.1.2 на стр. 72);

     примените доверенную зону: нажмите на кнопку **Режим защиты** и в диалоговом окне **Дополнительно** установите флажок **Применять доверенную зону** (о том, как сформировать доверенную зону, см. п. 20.7.3 на стр. 325);

     измените режим защиты объектов: нажмите на кнопку **Режим защиты** и в диалоговом окне **Дополнительно** выберите нужный режим защиты объектов (подробнее о параметре читайте в п. A.3.1 на стр. 399);

   - в задаче **Проверка скриптов** на закладке **Настройка**:

     выберите, разрешать или запрещать выполнение скриптов, которые Антивирус признает подозрительными;

     примените доверенную зону (о том, как сформировать доверенную зону, см. п. 20.7.3 на стр. 325);

- в задаче **Полная проверка** компьютера на закладке **Область проверки**:

  сформируйте область проверки (о предопределенных областях читайте в п. 9.2.1.2 на стр. 124);

  измените приоритет рабочего процесса, в котором будет выполняться задача (см. п. 9.3 на стр. 143);

  присвойте задаче статус «Задача полной проверки компьютера» (см. п. 21.4 на стр. 344);

  примените доверенную зону (о том, как сформировать доверенную зону, см. п. 20.7.3 на стр. 325);

- в задаче **Копирование обновлений**:

  на **закладке Настройка копирования обновлений** укажите состав обновлений и папку для их сохранения (см. п. A.5.7 на стр. 435);

  на закладке **Источник обновлений** укажите источник обновлений (см. п. A.5.1 на стр. 426);

- на закладке **Расписание** настройте расписание задачи (см. п. 5 инструкции по созданию задачи на стр. 339);

- на закладке **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача (см. п. 5.9.1 на стр. 64);

- на закладке **Уведомление** настройте уведомление о результатах выполнения задачи (подробнее читайте в документе *Kaspersky Administration Kit. Справочное Руководство*).

> **Примечание**
>
> Во время действия политики Kaspersky Administration Kit значения параметров, помеченные в политике значком 🔒 в диалоговом окне **Свойства задачи** Консоли администрирования не доступны для редактирования.

5. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **ОК** в диалоговом окне **Свойства задачи**, чтобы сохранить изменения.

21.4. Управление полной проверкой серверов. Присвоение задаче проверки по требованию статуса *Задача полной проверки компьютера*

По умолчанию Kaspersky Administration Kit присваивает серверу статус *Предупреждение*, если задача **Полная проверка компьютера** выполняется реже, чем указано параметром Антивируса **Порог формирования события «Полная проверка компьютера выполнялась давно»**.

Вы можете «управлять» полной проверкой всех серверов, входящих в одну группу администрирования, следующим образом:

1. Создайте групповую задачу проверки по требованию. В окне **Настройка** мастера создания задач присвойте ей статус «Задача полной проверки компьютера». Указанные вами параметры задачи – область проверки и параметры безопасности – будут едиными для всех серверов группы. Настройте расписание задачи. Подробнее о том, как создать задачу, читайте в п. 21.2 на стр. 332.

   Примечание

   Вы можете присвоить задаче проверки по требованию статус «Задача полной проверки компьютера» как при ее создании, так и позже, в диалоговом окне **Свойства задачи**.

2. С помощью новой или существующей политики отключите системную задачу **Полная проверка компьютера** на серверах группы (см. п. 19.4 на стр. 294).

С этого момента Сервер администрирования Kaspersky Administration Kit будет оценивать состояние безопасности защищаемого сервера и уведомлять вас о нем по результатам последнего выполнения задачи со статусом «Задача полной проверки компьютера», а не по результатам выполнения системной задачи **Полная проверка компьютера**.

Вы можете присваивать статус «Задача полной проверки компьютера» как групповым, так и глобальным задачам проверки по требованию.

В консоли Антивируса в ММС вы можете просмотреть, является ли групповая или глобальная задача проверки по требованию задачей полной проверки компьютера.

Примечание

В консоли Антивируса флажок **Считать выполнение задачи полной проверкой сервера** отображается в свойствах задач, но он не доступен для редактирования.

ЧАСТЬ 4. СЧЕТЧИКИ АНТИВИРУСА

В этой части содержится следующая информация:

- описание счетчиков производительности для приложения «Системный монитор» (Глава 22 на стр. 347);
- описание счетчиков и ловушек SNMP Антивируса (Глава 23 на стр. 358).

ГЛАВА 22. СЧЕТЧИКИ ПРОИЗВОДИТЕЛЬНОСТИ ДЛЯ ПРИЛОЖЕНИЯ «СИСТЕМНЫЙ МОНИТОР»

В этой главе содержится общая информация о счетчиках производительности Антивируса (см. п. 22.1 на стр. 348) и описание каждого из счетчиков:

- Общее количество отвергнутых запросов (см. п. 22.2 на стр. 349);
- Общее количество пропущенных запросов (см. п. 22.3 на стр. 350);
- Количество запросов, необработанных из-за нехватки системных ресурсов (см. п. 22.4 на стр. 351);
- Количество запросов, отданных на обработку (см. п. 22.5 на стр. 352);
- Среднее количество потоков диспетчера файловых перехватов (см. п. 22.6 на стр. 353);
- Максимальное количество потоков диспетчера файловых перехватов (см. п. 22.7 на стр. 354);
- Количество зараженных объектов в очереди на обработку (см. п. 22.8 на стр. 355);
- Количество объектов, обрабатываемых за секунду (см. п. 22.9 на стр. 357).

22.1. О счетчиках производительности Антивируса

Если в состав устанавливаемых компонентов Антивируса включен компонент **Счетчики производительности**, то во время установки Антивирус регистрирует свои счетчики производительности для приложения «Системный монитор» Microsoft Windows.

С помощью счетчиков Антивируса вы можете контролировать производительность Антивируса во время выполнения задач постоянной защиты. Вы можете обнаруживать узкие места при его совместной работе с другими приложениями и недостаточность ресурсов. Вы можете диагностировать неоптимальную настройку Антивируса и сбои в его работе.

Вы можете просматривать счетчики производительности Антивируса, открыв консоль **Производительность** в элементе **Администрирование Панели управления**.

В следующих пунктах приводятся определения счетчиков, рекомендуемые интервалы считывания показаний, пороговые значения и рекомендации по настройке Антивируса в случае, если значения счетчиков их превышают.

22.2. Общее количество отвергнутых запросов

Название	Общее количество отвергнутых запросов (Number of requests denied)
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были приняты рабочими процессами Антивируса; рассчитывается с момента последнего запуска Антивируса. Антивирус пропускает объекты, запросы на обработку которых отвергаются рабочими процессами Антивируса.
Назначение	Счетчик позволяет обнаруживать: • снижение качества постоянной защиты из-за полной загрузки рабочих процессов Антивируса; • прерывание постоянной защиты из-за отказа диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 ч
Рекомендации по настройке, если значение превышает пороговое	Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов. Возможны следующие ситуации в зависимости от «поведения» счетчика: • счетчик показывает несколько отвергнутых запросов в течение длительного времени: все рабочие процессы Антивируса были полностью загружены, поэтому Антивирусу не удалось проверить объекты. Чтобы исключить пропуск объектов, увеличьте количество процессов Антивируса для задач постоянной защиты. Вы можете использовать параметры Антивируса **Максимальное число активных процессов** (подробнее о параметре читайте в п. A.1.1 на стр. 373) и **Число процесссов для по-**

	стоянной защиты (подробнее о параметре читайте в п. A.1.2 на стр. 374); • количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Антивирус не проверяет объекты при доступе. Перезапустите Антивирус.

22.3. Общее количество пропущенных запросов

Название	Общее количество пропущенных запросов (Number of requests skipped)
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых процессом драйвера, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска Антивируса. Если запрос на обработку объекта, принятый одним из рабочих процессов, не отправил события о завершении обработки, драйвер передает этот запрос другому процессу и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1. Если драйвер перебрал все рабочие процессы и ни один из них не принял запрос на обработку (был занят) или не отправивших события о завершении обработки, то Антивирус пропускает такой объект и на 1 увеличивается значение счетчика **Общее количество отвергнутых запросов**.
Назначение	Счетчик позволяет обнаруживать снижение производительности из-за простоя потоков диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 ч

Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нулевого, то зависли и простаивают один или несколько потоков диспетчера файловых перехватов. Значение счетчика соответствует количеству потоков, простаивающих в текущий момент. Если скорость проверки не удовлетворительна, перезапустите Антивирус, чтобы восстановить простаивающие потоки.

22.4. Количество запросов, не обработанных из-за нехватки системных ресурсов

Название	Количество запросов, не обработанных из-за нехватки системных ресурсов (Number of requests not processed due to lack of resources)
Определение	Общее количество запросов драйвера файловых перехватов, не обработанных из-за нехватки системных ресурсов (например, оперативной памяти); рассчитывается с момента последнего запуска Антивируса. Антивирус пропускает объекты, запросы на проверку которых не обрабатываются драйвером файловых перехватов.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты, возникающее из-за недостаточности системных ресурсов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 ч
Рекомендации по настройке, если значение	Если значение счетчика отличается от нулевого, рабочие процессы Антивируса нуждаются в увеличении объема оперативной памяти для обработки запросов.

превышает пороговое	Возможно, активные процессы других приложений используют всю доступную оперативную память.

22.5. Количество запросов, отданных на обработку

Название	Количество запросов, отданных на обработку (Number of requests sent to be processed)
Определение	Количество объектов, ожидающих обработки рабочими процессами Антивируса в текущий момент
Назначение	Счетчик позволяет отслеживать загрузку рабочих процессов Антивируса и общий уровень файловой активности на сервере.
Нормальное / пороговое значение	Значение счетчика может колебаться в зависимости от уровня файловой активности на сервере
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	нет

22.6. Среднее количество потоков диспетчера файловых перехватов

Название	Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams)
Определение	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, среднее по всем процессам, занятым в задачах постоянной защиты в текущий момент
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты из-за полной загрузки процессов Антивируса
Нормальное / пороговое значение	Варьируется / 40
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	В каждом рабочем процессе может быть создано до 60 потоков диспетчера файловых перехватов. Если значение счетчика приближается к 60, возникает риск того, что ни одному из рабочих процессов не удастся принять на обработку очередной запрос от драйвера файловых перехватов и Антивирус пропустит объект. Увеличьте количество процессов Антивируса для задач постоянной защиты. Вы можете использовать параметры Антивируса **Максимальное число активных процессов** (подробнее о параметре читайте в п. A.1.1 на стр. 373) и **Число процесссов для постоянной защиты** (подробнее о параметре читайте в п. A.1.2 на стр. 374).

22.7. Максимальное количество потоков диспетчера файловых перехватов

Название	Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams)
Определение	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, наибольшее из всех процессов, занятых в задачах постоянной защиты в текущий момент
Назначение	Счетчик позволяет обнаруживать и устранять снижение производительности из-за неравномерного распределения нагрузки в выполняющихся рабочих процессах.
Нормальное / пороговое значение	Варьируется / 40
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение этого счетчика значительно и продолжительно превышает значение счетчика **Среднее количество потоков диспетчера файловых перехватов**, Антивирус неравномерно распределяет нагрузку на выполняющиеся процессы. Перезапустите Антивирус.

22.8. Количество зараженных объектов в очереди на обработку

Название	Количество зараженных объектов в очереди на обработку (Number of items in the infected object queue)
Определение	Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент
Назначение	Счетчик позволяет обнаруживать: • прерывание постоянной защиты из-за возможного отказа диспетчера файловых перехватов; • перегруженность процессора из-за неравномерного распределения процессорного времени между другими работающими приложениями и Антивирусом; • вирусную эпидемию.
Нормальное / пороговое значение	Значение счетчика может быть отличным от нуля, пока Антивирус обрабатывает обнаруженные зараженные или подозрительные объекты, но оно возвращается к нулю вскоре после окончания обработки / Значение счетчика остается ненулевым длительное время.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика остается ненулевым длительное время: • Антивирус не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов); Перезапустите Антивирус. • не достаточно процессорного времени для обработки объектов; Обеспечьте выделение Антивирусу дополнительного процессорного времени, например, снизив нагрузку на сервер другими приложениями.

	• возникла вирусная эпидемия. Вы можете включить функцию *Предотвращение вирусных эпидемий* (см. п. 7.5 на стр. 101). О возникновении вирусной эпидемии также говорит большое количество обнаруженных зараженных или подозрительных объектов в задаче **Постоянная защита файлов**. Вы можете просмотреть информацию о количестве обнаруженных объектов в статистике задачи (см. п. 6.3 на стр. 90) или подробном отчете о выполнении задачи (см. п. 13.2.4 на стр. 209).

22.9. Количество объектов, обрабатываемых за секунду

Название	Количество объектов, обрабатываемых за секунду (Number of objects processed per second)
Определение	Количество обработанных объектов, разделенное на количество времени, в течение которого эти объекты были обработаны; рассчитывается за равные промежутки времени
Назначение	Счетчик отражает скорость обработки объектов; позволяет обнаружить и устранить снижение производительности сервера, возникшее из-за недостаточности выделяемого рабочим процессам Антивируса процессорного времени или сбоя в работе Антивируса.
Нормальное / пороговое значение	Варьируется / Нет
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Значения счетчика зависят от установленных значений параметров Антивируса и загрузки сервера процессами других приложений. Наблюдайте средний уровень показаний счетчика в течение продолжительного времени. Если общий уровень показаний счетчика снизился: • рабочим процессам Антивируса не хватает процессорного времени для обработки объектов; Обеспечьте выделение Антивирусу дополнительного процессорного времени, например, снизив нагрузку на сервер другими приложениями. • возник сбой в работе Антивируса (простаивает несколько потоков). Перезапустите Антивирус.

ГЛАВА 23. СЧЕТЧИКИ И ЛОВУШКИ SNMP АНТИВИРУСА

В этой главе содержится следующая информация:

- о счетчиках и ловушках SNMP Антивируса (см. п. 23.1 на стр. 358);
- описание счетчиков SNMP (см. п. 23.2 на стр. 358);
- описание ловушек SNMP (см. п. 23.3 на стр. 363).

23.1. О счетчиках и ловушках SNMP Антивируса

Если вы включили в состав устанавливаемых компонентов Антивируса компонент **Счетчики и ловушки SMNP**, вы можете просматривать счетчики и ловушки Антивируса по протоколам Simple Network Management Protocol (SNMP) и HP Open View.

Чтобы просматривать счетчики и ловушки Антивируса на компьютере-рабочем месте администратора, запустите на защищаемом сервере Службу SNMP (SNMP Service), а на рабочем месте администратора – Службу SNMP (SNMP Service) и Службу ловушек SNMP (SNMP Trap Service).

23.2. Счетчики SNMP Антивируса

В Антивирусе предусмотрены следующие счетчики SNMP:

- счетчики производительности (см. п. 23.2.1 на стр. 359);
- общие счетчики (см. п. 23.2.2 на стр. 359);
- счетчик обновления (см. п. 23.2.3 на стр. 360);
- счетчики постоянной защиты (см. п. 23.2.4 на стр. 360);
- счетчики карантина (см. п. 23.2.5 на стр. 362);
- счетчики резервного хранилища (см. п. 23.2.6 на стр. 362);

- счетчики блокирования доступа с компьютеров к серверу (см. п. 23.2.7 на стр. 362);
- счетчики проверки скриптов (см. п. 23.2.8 на стр. 363).

23.2.1. Счетчики производительности

Счетчик	Определение
currentRequestsAmount	Количество запросов, отданных на обработку (см. описание в п. 22.5 на стр. 352)
currentInfectedQueueLength	Количество зараженных объектов в очереди на обработку (см. описание в п. 22.8 на стр. 355)
currentObjectProcessingRate	Количество объектов, обрабатываемых за секунду (см. описание в п. 22.9 на стр. 357)
currentWorkProcessesAmount	Количество рабочих процессов Антивируса в текущий момент

23.2.2. Общие счетчики

Счетчик	Определение
currentApplicationUptime	Время работы Антивируса с момента его последнего запуска, в сотых долях секунды
currentFileMonitorTaskStatus	Состояние задачи **Постоянная защита файлов**: On – выполняется; Off – остановлена или приостановлена
currentScriptCheckerTaskStatus	Состояние задачи **Проверка скриптов**: On – выполняется; Off – остановлена или приостановлена
lastFullScanAge	«Возраст» последней полной проверки сервера (промежуток времени в секундах между датой завершения задачи, имеющей статус *задача полной проверки компьютера*, и текущим моментом)

Счетчик	Определение
licenseExpirationDate	Дата окончания срока действия ключа (если установлены активный и резервный ключи, то это дата показывает, когда заканчивается суммарный срок действия активного и резервного ключей)

23.2.3. Счетчик обновления

Счетчик	Определение
avBasesAge	«Возраст» баз (промежуток времени в сотых долях секунды между датой создания последних установленных обновлений баз и текущим моментом).

23.2.4. Счетчики постоянной защиты

Счетчик	Определение
totalObjectsProcessed	Общее количество проверенных объектов с момента последнего запуска задачи **Постоянная защита файлов**
totalInfectedObjectsFound	Общее количество обнаруженных зараженных объектов с момента последнего запуска задачи **Постоянная защита файлов**
totalSuspiciousObjectsFound	Общее количество обнаруженных подозрительных объектов с момента последнего запуска задачи **Постоянная защита файлов**
totalVirusesFound	Общее количество обнаруженных угроз с момента последнего запуска задачи **Постоянная защита файлов**

Счетчик	Определение
totalObjectsQuarantined	Общее количество зараженных или подозрительных объектов, которые Антивирус поместил на карантин; рассчитывается с момента последнего запуска задачи **Постоянная защита файлов**
totalObjectsNotQuarantined	Общее количество зараженных или подозрительных объектов, которые Антивирус пытался поместить на карантин, но это ему не удалось; рассчитывается с момента последнего запуска задачи **Постоянная защита файлов**
totalObjectsDisinfected	Общее количество зараженных объектов, которые Антивирус вылечил; рассчитывается с момента последнего запуска задачи **Постоянная защита файлов**
totalObjectsNotDisinfected	Общее количество зараженных объектов, которые Антиврус пытался вылечить, но это ему не удалось; рассчитывается с момента последнего запуска задачи **Постоянная защита файлов**
totalObjectsDeleted	Общее количество зараженных или подозрительных объектов, которые Антивирус удалил; рассчитывается с момента последнего запуска задачи **Постоянная защита файлов**
totalObjectsNotDeleted	Общее количество зараженных или подозрительных объектов, которые Антивирус должен был удалить, но это ему не удалось; рассчитывается с момента последнего запуска задачи **Постоянная защита файлов**
totalObjectsBackedUp	Общее количество зараженных объектов, которые Антивирус поместил в резервное хранилище; рассчитывается с момента последнего запуска задачи **Постоянная защита файлов**

Счетчик	Определение
totalObjectsNotBackedUp	Общее количество зараженных объектов, которые Антивирус пытался поместить в резервное хранилище, но это ему не удалось; рассчитывается с момента последнего запуска задачи **Постоянная защита файлов**

23.2.5. Счетчики карантина

Счетчик	Определение
totalObjects	Количество объектов в папке карантина в текущий момент
totalSuspiciousObjects	Количество подозрительных объектов в папке карантина в текущий момент
currentStorageSize	Объем данных в папке карантина (МБ)

23.2.6. Счетчики резервного хранилища

Счетчик	Определение
currentBackupStorageSize	Объем данных в папке резервного хранилища (МБ)

23.2.7. Счетчики блокирования доступа с компьютеров к серверу

Счетчик	Определение
currentHostsBlocked	Количество компьютеров в списке блокирования

Счетчик	Определение
totalNotBlocked	Количество невыполненных операций блокирования доступа с компьютеров, исключенных из блокирования (доверенных компьютеров), с момента включения функции автоматического блокирования

23.2.8. Счетчики проверки скриптов

Счетчик	Определение
totalScriptsProcessed	Общее количество проверенных скриптов
totalInfectedIDangerous-ScriptsFound	Общее количество обнаруженных зараженных скриптов
totalSuspiciousScriptsFound	Общее количество обнаруженных подозрительных скриптов
totalScriptsBlocked	Общее количество скриптов, доступ к которым был заблокирован

23.3. Ловушки SNMP

В следующей таблице описаны ловушки SNMP Антивируса; параметры ловушек описаны в таблице ниже.

Ловушка	Описание	Параметры
eventThreatDetected	Обнаружена угроза. Подробнее о том, как Антивирус обнаруживает зараженные и подозрительные объекты, читайте в п. 1.1.3 на стр. 20.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty

Ловушка	Описание	Параметры
eventBackupStorageSizeExceeds	Превышен максимальный размер резервного хранилища. Общий объем данных в папке резервного хранилища превысил значение, указанное параметром **Максимальный размер резервного хранилища**. Антивирус продолжает резервировать зараженные объекты.	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	Достигнут порог свободного места в резервном хранилище. Размер свободного пространства в папке резервного хранилища, заданный параметром **Порог свободного места в резервном хранилище**, уменьшился до указанного значения. Антивирус продолжает резервировать зараженные объекты.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, указанное параметром **Максимальный размер карантина**. Антивирус продолжает помещать подозрительные объекты на карантин.	eventDateAndTime eventSeverity eventSource

Ловушка	**Описание**	**Параметры**
eventThresholdQuarantineStorageSizeExceeds	Достигнут порог свободного места в карантине. Размер свободного пространства в папке карантина, заданный параметром **Порог свободного места в карантине**, уменьшился до указанного значения. Антивирус продолжает помещать подозрительные объекты на карантин.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Ошибка помещения объекта на карантин	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Ошибка сохранения копии объекта в резервном хранилище	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Возникла ошибка хранилища карантина.	eventSeverity eventDateAndTime eventSource eventReason

Ловушка	Описание	Параметры
eventBackupInternalError	Возникла ошибка резервного хранилища.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	Базы устарели. Рассчитывается количество дней, прошедших с момента последнего завершения задачи обновления баз (локальной, групповой или глобальной).	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	Базы сильно устарели. Рассчитывается количество дней, прошедших с момента последнего завершения задачи обновления баз (локальной, групповой или глобальной).	eventSeverity eventDateAndTime eventSource days
eventApplicationModulesIntegrityFailed	Возникла ошибка проверки целостности модулей приложения	eventSeverity eventDateAndTime eventSource
eventApplicationStarted	Антивирус запущен.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Антивирус остановлен.	eventSeverity eventDateAndTime eventSource
eventFullScanWasntPerformForALongTime	Полная проверка проводилась давно. Рассчитывается количество дней с момента последнего завершения задачи, имеющей статус *Задача полной проверки компьютера*	eventSeverity eventDateAndTime eventSource days

Ловушка	Описание	Параметры
eventLicenseHasExpired	Срок действия ключа истек.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	Срок действия ключа скоро истечет. Рассчитывается количество дней, оставшихся до окончания срока действия ключа	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Ошибка выполнения задачи	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Ошибка выполнения задачи обновления	eventSeverity eventDateAndTime taskName updaterErrorEventReason

В следующей таблице описаны параметры ловушек и возможные значения параметров.

Параметр	Описание и возможные значения
eventDateAndTime	Время возникновения события
eventSeverity	Уровень важности события. Возможные значения включают: • critical (1) – критический, • warning (2) – предупреждение, • info (3) – информационный.
UserName	Имя пользователя (например, пользователя, который пытался получить доступ к зараженному файлу)

Параметр	Описание и возможные значения
computerName	Имя компьютера (например, компьютера, с которого пользователь пытался получить доступ к зараженному файлу)
eventSource	Источник события: функциональный компонент, в работе которого возникло событие. Возможные значения включают: • unknown (0) – функциональный компонент не определен; • quarantine (1) – Карантин; • backup (2) – Резервное хранилище; • reporting (3) – Отчеты; • updates (4)– Обновление; • realTimeProtection (5) –Постоянная защита; • onDemandScanning (6) – Проверка по требованию; • product (7) – событие связано не с работой отдельных компонентов, а с работой Антивируса в целом; • systemAudit (8) – Журнал системного аудита; • hostBlocker (9) – Блокирование доступа с компьютеров к серверу.
eventReason	Причина возникновения события. Возможные значения включают: • reasonUnknown (0) – причина не определена, • reasonInvalidSettings (1) – только для событий резервного хранилища и карантина; отображается, если недоступна папка карантина или папка резервного хранилища (недостаточно прав для доступа или папка неверно указана в параметрах карантина, например, указан сетевой путь). В этом случае Антивирус будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.
objectName	Имя объекта (например, имя файла, в котором обнаружена угроза)
threatName	Имя угрозы

Параметр	Описание и возможные значения
detectType	Тип угрозы. Возможные значения включают: • undefined (0) – не определена; • virware – классические вирусы и сетевые черви; • trojware – троянские программы; • malware – прочие вредоносные программы; • adware – программы-рекламы; • pornware – программы порнографического содержания; • riskware – потенциально опасные приложения. Подробнее о типах угроз читайте в п. 1.1.2 на стр. 16.
detectCertainty	Степень уверенности обнаружения угрозы. Возможные значения включают: • Warning (предупреждение) – объект признан подозрительным с использованием эвристического анализатора; • Suspicion (подозрительный) – объект признан подозрительным: обнаружено частичное совпадение участка кода объекта с участком кода известной угрозы; • Sure (зараженный) – объект признан зараженным: обнаружено полное совпадение участка кода объекта с участком кода известной угрозы.
days	Количество дней (например, количество дней до окончания срока действия ключа)
errorCode	Код ошибки
knowledgeBaseId	Адрес статьи в базе знаний (например, адрес статьи, описывающей какую-либо ошибку)
taskName	Имя задачи

Параметр	Описание и возможные значения
updaterErrorEventReason	Причина неприменения обновления. Возможные значения включают: • reasonUnknown(0) – причина не определена; • reasonAccessDenied – доступ запрещен; • reasonUrlsExhausted – список источников обновлений исчерпан; • reasonInvalidConfig – неправильный файл конфигурации; • reasonInvalidSignature – неверная подпись; • reasonCantCreateFolder – невозможно создать папку; • reasonFileOperError – файловая ошибка; • reasonDataCorrupted – объект поврежден; • reasonConnectionReset – сброс соединения; • reasonTimeOut – истекло время ожидания при соединении; • reasonProxyAuthError – ошибка проверки подлинности на прокси-сервере; • reasonServerAuthError – ошибка проверки подлинности на сервере; • reasonHostNotFound – компьютер не найден; • reasonServerBusy – сервис недоступен; • reasonConnectionError – ошибка соединения; • reasonModuleNotFound – объект на найден; • reasonBlstCheckFailed(16) – ошибка проверки списка отозванных лицензий. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут. Смотрите описание этих причин и возможные действия администратора на сайте Службы технической поддержки в разделе **Если программа выдала ошибку** (http://support.kaspersky.ru/error).

Параметр	Описание и возможные значения
storageObjectNotAddedEventReason	Причина непомещения объекта в резервное хранилище или на карантин. Возможные значения включают: • reasonUnknown(0) – причина не определена; • reasonStorageInternalError – ошибка базы данных; восстановите Антивирус; • reasonStorageReadOnly – база данных доступна только для чтения; восстановите Антивирус; • reasonStorageIOError – ошибка ввода-вывода: а) Антивирус поврежден, восстановите Антивирус; б) диск, на котором хранятся файлы Антивируса, поврежден; • reasonStorageCorrupted – хранилище повреждено; восстановите Антивирус; • reasonStorageFull – база данных полна; освободите место на диске; • reasonStorageOpenError – не удалось открыть файл базы данных; восстановите Антивирус; • reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Антивируса; • reasonObjectNotFound – помещаемый в хранилище объект отсутствует на диске; • reasonObjectAccessError – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator. • reasonDiskOutOfSpace – недостаточно места на диске.

ПРИЛОЖЕНИЕ А. ОПИСАНИЕ ОБЩИХ ПАРАМЕТРОВ АНТИВИРУСА, ПАРАМЕТРОВ ЕГО ФУНКЦИЙ И ЗАДАЧ

А.1. Общие параметры Антивируса

Вы можете настроить следующие общие параметры Антивируса:

- максимальное число активных процессов (см. п. А.1.1 на стр. 373);
- количество процессов для постоянной защиты (см. п. А.1.2 на стр. 374);
- количество процессов для фоновых задач проверки по требованию (см. п. А.1.3 на стр. 376);
- восстановление задач (см. п. А.1.4 на стр. 377);
- срок хранения информации, которая отображается в узле **Отчеты** (см. п. А.1.5 на стр. 378);
- срок хранения информации, которая отображается в узле **Журнал системного аудита** (см. п. А.1.6 на стр. 379);
- действия при переходе на питание от источника бесперебойного питания (см. п. А.1.7 на стр. 379);
- пороги формирования событий (см. п. А.1.8 на стр. 380);
- создание журнала трассировки (см. п. А.1.9 на стр. 381);
- создание файлов дампов памяти процессов Антивируса (см. п. А.1.10 на стр. 388).

A.1.1. Максимальное число активных процессов

<table>
<tr><td>Параметр</td><td>Максимальное число активных процессов.</td></tr>
<tr><td>Описание</td><td>Этот параметр относится к группе параметров Масштабируемость Антивируса. Он устанавливает максимальное количество рабочих процессов, которые Антивирус может запустить одновременно.

В рабочих процессах Антивируса выполняются задачи постоянной защиты, проверки по требованию и обновления.

Увеличение количества параллельно работающих процессов повышает скорость проверки файлов и устойчивость Антивируса к сбоям. Однако высокое значение этого параметра может снизить общую производительность сервера и повысить потребление оперативной памяти.

Примечание

Обратите внимание, что в Консоли Администрирования приложения Kaspersky Administration Kit вы можете устанавливать параметр Максимальное число активных процесссов только для Антивируса на отдельном сервере (в диалоговом окне Параметры приложения); вы не можете изменять этот параметр в свойствах политики для группы серверов.</td></tr>
<tr><td>Возможные значения</td><td>1– 8</td></tr>
<tr><td>Значение по умолчанию</td><td>Антивирус выполняет масштабирование автоматически в зависимости от количества процессоров на сервере:

<table><tr><th>Количество процессоров</th><th>Максимальное число активных процессов</th></tr><tr><td>=1</td><td>1</td></tr><tr><td>1 < кол-во процессоров < 4</td><td>2</td></tr><tr><td>≥ 4</td><td>4</td></tr></table></td></tr>
</table>

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;

- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.2. Число процессов для постоянной защиты

Параметр	Число процессов для постоянной защиты.
Описание	Этот параметр относится к группе параметров **Масштабируемость** Антивируса. С помощью этого параметра вы можете устанавливать фиксированное количество процессов, в которых Антивирус будет выполнять задачи постоянной защиты. Более высокое значение этого параметра повысит скорость проверки объектов в задачах постоянной защиты. Однако, чем больше рабочих процессов задействует Антивирус, тем больше будет его влияние на общую производительность защищаемого сервера и его потребление оперативной памяти. **Примечание** Обратите внимание, что в Консоли Администрирования приложения Kaspersky Administration Kit вы можете устанавливать параметр **Число процессов для постоянной защиты** только для Антивируса на отдельном сервере (в диалоговом окне **Параметры приложения**); вы не можете изменять этот параметр в свойствах политики для группы серверов.
Возможные значения	Возможные значения: 1-N, где N – значение, заданное параметром **Максимальное число активных процессов**. Если вы установите **Число процессов для постоянной защиты** равным **Максимальному числу активных процессов**, вы снизите влияние Антивируса на скорость файлового обмена компьютеров с сервером, еще повысив его быстродействие во время постоянной защиты. Однако задачи обновления и задачи проверки по требованию с базовым приоритетом **Средний** (**Normal**) будут выполняться в уже запущенных рабочих процессах Антивируса. Задачи проверки по требованию будут выполняться медленнее. А если выполнение задачи вызовет аварийное завершение процесса, на его перезапуск потребуется больше времени. Задачи проверки по требованию с базовым приоритетом **Низкий** (**Low**) всегда выполняются в отдельном процессе или

<table>
<tr><td></td><td>процессах (см. п. A.1.3 на стр. 376).</td></tr>
<tr><td>Значение по умолчанию</td><td>Антивирус выполняет масштабирование автоматически в зависимости от количества процессоров на сервере:
<table>
<tr><th>Количество процессоров</th><th>Число процессов для постоянной защиты</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>> 1</td><td>2</td></tr>
</table></td></tr>
</table>

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.3. Число процессов для фоновых задач проверки по требованию

Параметр	Число процессов для фоновых задач проверки по требованию.
Описание	Этот параметр относится к группе параметров **Масштабируемость** Антивируса. С помощью этого параметра вы можете устанавливать максимальное количество процессов, в которых Антивирус будет выполнять задачи проверки по требованию в фоновом режиме. Количество процессов, которое вы устанавливаете этим параметром, не входит в общее количество рабочих процессов Антивируса, заданное параметром **Максимальное количество активных процессов**. Например, если вы установите: • максимальное количество активных процессов – 3; • количество процессов для задач постоянной защиты – 3; • количество процессов для фоновых задач проверки по требованию – 1; а затем запустите задачи постоянной защиты и одну задачу проверки по требованию в фоновом режиме, то общее количество рабочих процессов kavfswp.exe Антивируса составит 4. В одном рабочем процессе с низким приоритетом может выполняться несколько задач проверки по требованию. Вы можете повысить количество рабочих процессов, например, если вы запускаете одновременно несколько задач в фоновом режиме, чтобы выделить отдельный процесс для каждой задачи. Выделение отдельных процессов для задач повышает надежность выполнения этих задач и их скорость.
Возможные значения	1-4
Значение по умолчанию	1

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.4. Восстановление задач

Параметр	Восстановление задач (**Выполнять восстановление задач**).
Описание	Этот параметр относится к группе параметров **Надежность** Антивируса. Он включает восстановление задач, если они завершаются аварийно, и устанавливает количество попыток восстановления задач проверки по требованию. Когда задача завершается аварийно, процесс kavfs.exe Антивируса пытается повторно запустить процесс, в котором эта задача выполнялась в момент завершения. *Если восстановление задач выключено*, Антивирус не восстанавливает задачи постоянной защиты и проверки по требованию. *Если восстановление задач включено*, Антивирус пытается восстановить задачи постоянной защиты, пока они не будут успешно запущены, и пытается восстановить задачи проверки по требованию столько раз, сколько указано этим параметром.
Возможные значения	Включено / выключено. Количество попыток восстановления задач проверки по требованию: 1-10.
Значение по умолчанию	Восстановление задач включено. Количество попыток восстановления задач проверки по требованию – 2.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.5. Срок хранения отчетов

Параметр	Срок хранения отчетов (**Хранить отчеты и события не более … дней**).
Описание	Этот параметр определяет, сколько дней будут храниться сводные и подробные отчеты о выполнении задач, которые отображаются в консоли Антивируса в ММС в узле **Отчеты**. Вы можете выключить этот параметр, чтобы хранить отчеты о выполнении задач неограниченное время. В этом случае файл отчета может достигнуть большого размера.
Возможные значения	1–365
Значение по умолчанию	В подробных отчетах о выполнении задач Антивирус удаляет записи о событиях, возникших более 30 дней назад. Сводные отчеты о завершенных задачах удаляются через 30 дней после завершения задач.

О том, как настроить параметр:

- в консоли Антивируса в ММС, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.6. Срок хранения событий в журнале системного аудита

Параметр	Срок хранения журнала системного аудита (**Хранить события не более … дней**).
Описание	Вы можете ограничить срок хранения событий, которые отображаются в узле **Журнал системного аудита** консоли Антивируса в MMC.
Возможные значения	1–365
Значение по умолчанию	События из журнала системного аудита не удаляются.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.7. Действия при работе от источника бесперебойного питания

Параметр	Использование источника бесперебойного питания.
Описание	Этот параметр определяет действия, которые Антивирус выполнит, когда сервер перейдет на питание от источника бесперебойного питания.
Возможные значения	• запускать / не запускать задачи проверки по требованию, которые должны быть запущены по расписанию; • выполнять / останавливать все выполняемые задачи проверки по требованию.
Значение по умолчанию	По умолчанию при работе сервера от источника бесперебойного питания Антивирус: • не запускает задачи проверки по требованию, которые должны быть запущены по расписанию;

	• автоматически останавливает все выполняемые задачи проверки по требованию.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.8. Пороги формирования событий

Параметр	Пороги формирования событий.
Описание	Вы можете указать пороги формирования событий следующих трех типов: • *Базы устарели* и *Базы сильно устарели*. Событие возникает, если базы Антивируса не обновляются в течение указанного параметром количества дней с момента создания последних установленных обновлений баз. Вы можете настроить уведомление администратора по этим событиям. • *Полная проверка компьютера выполнялась давно*. Событие возникает, если в течение указанного количества дней не выполняется ни одна из задач, отмеченных флажком **Считать выполнение задачи полной проверкой компьютера**. Подробнее о статусе «задача полной проверки компьютера» читайте в п. 21.4 на стр. 344.
Возможные значения	Количество дней от 1 до 365.
Значение по умолчанию	*Базы устарели* – 7 дней; *Базы сильно устарели* – 14 дней; *Полная проверка компьютера выполнялась давно* – 30 дней.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.9. Параметры журнала трассировки

- создание журнала трассировки (см. п. A.1.9.1 на стр. 381);
- папка с файлами журнала трассировки (см. п. A.1.9.2 на стр. 383);
- уровень детализации журнала трассировки (см. п. A.1.9.3 на стр. 384);
- размер одного файла журнала трассировки (см. п. A.1.9.4 на стр. 385);
- трассировка только некоторых подсистем Антивируса (см. п. A.1.9.5 на стр. 386).

A.1.9.1. Создание журнала трассировки

Параметр	Создание журнала трассировки (**Записывать отладочную информацию в файл**).
Описание	Параметр **Создание журнала трассировки** относится группе параметров **Диагностика сбоев**. Если в работе Антивируса возникла проблема (например, Антивирус или отдельная задача завершается аварийно или не запускается) и вы ее хотите диагностировать, вы можете создать журнал трассировки и отправить файлы журнала на анализ в Службу технической поддержки «Лаборатории Касперского». Подробнее о том, как обратиться в Службу технической поддержки, читайте в п. 1.2.3 на стр. 24. Журнал трассировки каждого процесса Антивируса сохраняется в отдельный файл.
Значения и некоторые рекомендации по их использованию	Журнал трассировки создается / не создается. Чтобы включить создание журнала трассировки, вам нужно указать папку, в которой будут сохранены файлы журнала. Если вы управляете Антивирусом на защищаемом сервере через консоль, установленную на другом компьютере, то, чтобы включить ведение журнала трассировки подсистемы **gui**, вам нужно указать параметры журнала трассировки в реестре Microsoft Windows этого компьютера, а затем закрыть и снова открыть консоль Антивируса в MMC. • Если на компьютере установлена Microsoft Windows 32-разрядной версии: `HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVFSE`

	E\6.0\Trace\Configuration=sub-system=gui;level=info;sink=folder(<папка для файлов журнала трассировки и путь к ней>);roll=50000;layout=basic;logging=on • Если на компьютере установлена Microsoft Windows 64-разрядной версии: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\Trace\Configuration=sub-system=gui;level=info;sink=folder(<папка для файлов журнала трассировки и путь к ней>);roll=50000;layout=basic;logging=on Указывая путь к папке, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
По умолчанию	Журнал трассировки не создается.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.9.2. Папка с файлами журнала трассировки

Параметр	Папка с файлами журнала трассировки (**Папка файлов отладки**).
Описание	Чтобы включить создание журнала трассировки, вам нужно указать папку, в которой будут сохранены файлы журнала.
Значения и некоторые рекомендации по их использованию	Укажите папку на локальном диске защищаемого сервера. Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Не используйте в качестве папки для записи журнала трассировки папки на сетевых дисках сервера или дисках, созданных с помощью команды SUBST. Если вы управляете Антивирусом на защищаемом сервере через консоль MMC, установленную на удаленном рабочем месте администратора, то вы должны входить в группу локальных администраторов на защищаемом сервере, чтобы просматривать папки на нем. Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
Значение по умолчанию	Не указана.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.9.3. Уровень детализации журнала трассировки

Параметр	Уровень детализации журнала трассировки.
Описание	Вы можете выбрать уровень детализации журнала трассировки (*Отладочная информация*, *Информационные события*, *Важные события*, *Ошибки* или *Критические события*).
Значения и некоторые рекомендации по их использованию	Наиболее подробным является уровень *Отладочная информация*, при котором в журнал записываются все события, а наименее подробным является уровень *Критические события*, при котором в журнал записываются только критические события. Обратите внимание, что журнал трассировки может занимать большой объем дискового пространства.
Значение по умолчанию	Если, включив создание журнала трассировки, вы не измените параметры журнала, Антивирус будет трассировать подсистемы Антивируса с уровнем детализации *Отладочная информация*.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.9.4. Размер одного файла журнала трассировки

Параметр	Размер одного файла журнала трассировки.
Описание	Вы можете изменить максимальный размер одного файла журнала.
Значения и некоторые рекомендации по их использованию	1–999 МБ. Как только размер файла журнала достигнет максимального значения, Антивирус начнет записывать информацию в новый файл; предыдущий файл журнала сохранится.
Значение по умолчанию	Если, включив создание журнала трассировки, вы не измените параметры журнала, то максимальный размер одного файла журнала будет составлять 50 МБ.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.1.9.5. Трассировка отдельных подсистем Антивируса

Параметр	Трассировка только некоторых подсистем Антивируса.
Описание	Вы можете вести журнал не всех, а только некоторых подсистем Антивируса.
Значения и некоторые рекомендации по их использованию	В диалоговом окне настройки параметров Антивируса в группе параметров **Диагностика сбоев** нажмите на кнопку **Дополнительно** и в диалоговом окне **Дополнительная настройка** в поле **Отлаживаемые компоненты** введите коды подсистем, которые вы хотите трассировать. Разделяйте коды подсистем запятой. При вводе кодов подсистем соблюдайте регистр. Коды и названия подсистем Антивируса приводятся в таблице 29 на стр. 387. Антивирус применяет параметры трассировки подсистемы **gui** (оснастка Антивируса) после перезапуска консоли Антивируса; параметры трассировки подсистемы AK_conn (подсистема интеграции с Агентом администрирования Kaspersky Administration Kit) – после перезапуска Агента администрирования Kaspersky Administration Kit; параметры трассировки остальных подсистем Антивируса – сразу после сохранения параметров.
Значение по умолчанию	Если, включив создание журнала трассировки, вы не измените параметры журнала, то Антивирус будет трассировать все подсистемы Антивируса.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

В следующей таблице приводится список кодов подсистем Антивируса, информацию о которых вы можете добавлять в журнал трассировки.

Таблица 29. Список кодов подсистем для добавления в журнал трассировки

Код подсистемы	**Название подсистемы**
*	Все подсистемы (по умолчанию)
gui	Оснастка Антивируса в MMC
AK_conn	Подсистема интеграции с Агентом администрирования Kaspersky Administration Kit
bl	Управляющий процесс; реализует задачи управления Антивирусом
wp	Рабочий процесс; реализует задачи антивирусной защиты
blgate	Процесс удаленного управления Антивирусом
ods	Подсистема проверки по требованию
oas	Подсистема постоянной защиты файлов
qb	Подсистема карантина и резервного хранилища
scandll	Вспомогательный модуль антивирусной проверки
core	Подсистема базовой антивирусной функциональности
avscan	Подсистема антивирусной обработки
avserv	Подсистема управления антивирусным ядром
prague	Подсистема базовой функциональности
scsrv	Подсистема диспетчеризации запросов от перехватчика скриптов
script	Перехватчик скриптов
updater	Подсистема обновления баз и программных модулей

A.1.10. Создание файлов дампов памяти процессов Антивируса

Параметр	Создание файлов дампов памяти процессов Антивируса (**Создавать во время сбоя файлы дампов памяти**).
Описание	Параметр **Создание файлов дампов памяти процессов Антивируса** относится к группе параметров **Диагностика сбоев**. Если в работе Антивируса возникла проблема (например, Антивирус завершается аварийно) и вы хотите диагностировать ее, вы можете включить создание файлов дампов памяти процессов Антивируса и отправить эти файлы на анализ в Службу технической поддержки «Лаборатории Касперского». Подробнее о том, как обратиться в Службу технической поддержки, читайте в п. 1.2.3 на стр. 24.

Значения и некоторые рекомендации по их использованию	Файлы дампов создаются / не создаются.
	Чтобы включить создание файлов дампов, укажите папку, в которой файлы дампов будут сохранены.
	Примечание
	Если вы укажете путь к несуществующей папке, файлы дампов не будут созданы.
	Если вы управляете Антивирусом на защищаемом сервере через консоль Антивируса в MMC, установленную на другом компьютере, то, чтобы включить создание дампов процесса консоли Антивируса, вам нужно указать параметры создания дампов в реестре Microsoft Windows этого компьютера, а затем закрыть и снова открыть консоль Антивируса.
	• Если на компьютере установлена Microsoft Windows 32-разрядной версии:
	`HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\6.0\CrashDump\Enable=0x00000000`
	`HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\6.0\CrashDump\Folder=C:\Temp`
	• Если на компьютере установлена Microsoft Windows 64-разрядной версии:
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\CrashDump\Enable=0x00000000`
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\Kaspersk`

	yLab\KAVFSEE\6.0\CrashDump\Folder=C:\Temp 0x00000000 – выключить создание файлов дампов процесса консоли Антивируса в ММС; 0x00000001 – включить создание файлов дампов процесса консоли Антивируса в ММС. Folder=C:\Temp – папка, в которой будет сохранен файл дампов процесса консоли Антивируса в ММС при ее аварийном завершении. Указывая путь к папке с файлами дампов, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
Значение по умолчанию	Файлы дампов не создаются.

О том, как настроить параметр:

- в консоли Антивируса в ММС, см. п. 3.2 на стр. 46;
- в приложении Kaspersky Administration Kit, см. п. 20.2 на стр. 300.

A.2. Параметры расписания задач

Вы можете настроить следующие параметры расписания задач.

- частота запуска (см. п. A.2.1 на стр. 390);
- дата начала действия расписания и время запуска задачи (см. п. A.2.2 на стр. 392);
- дата окончания действия расписания (см. п. A.2.3 на стр. 393);
- максимальная продолжительность выполнения задачи (см. п. A.2.4 на стр. 394);
- промежуток времени в пределах суток, в течение которого задача будет приостановлена (см. п. A.2.5 на стр. 395);
- запуск пропущенных задач (см. п. A.2.6 на стр. 396);
- распределение времени запуска в интервале, мин. (см. п. A.2.7 на стр. 397).

A.2.1. Частота запуска

Параметр	Частота запуска.
Описание	Этот параметр является обязательным. Задача может запускаться с частотой в указанное вами количество часов, дней или недель, по указанным дням недели, после запуска Антивируса, обновления баз или получения обновлений Сервером администрирования.
Значения и некоторые рекомендации по их использованию	Возможные значения включают: • **Ежечасно**. Задача будет запускаться с периодичностью в заданное вами количество часов. • **Ежедневно**. Задача будет запускаться с периодичностью в заданное вами количество дней. • **Еженедельно**. Задача будет запускаться с периодичностью в заданное вами количество недель, по указанным дням недели. • **При запуске приложения**. Задача будет запускаться при каждом запуске Антивируса. • **После обновления баз** (этот вариант не применяется в

	задачах обновления). Задача будет запускаться после каждого обновления баз Антивируса. • **После получения обновлений Сервером администрирования** (применяется только в задачах **Обновление баз приложения**, **Обновление модулей приложения** и **Копирование обновлений**, отображается только в Консоли администрирования Kaspersky Administration Kit, не отображается в консоли Антивируса в MMC). Задача будет запускаться каждый раз, как только Сервер администрирования получит обновления баз.
Значение по умолчанию	В локальных системных задачах параметр **Частота запуска** по умолчанию имеет следующие значения: • Постоянная защита файлов – При запуске приложения; • Проверка скриптов – При запуске приложения; • Проверка при старте системы – При запуске приложения; • Проверка целостности приложения – При запуске приложения; • Полная проверка компьютера – Еженедельно (по пятницам в 20:00); • Проверка объектов на карантине – После обновления баз; • Обновление баз приложения – Каждый час; • Обновление модулей приложения – Еженедельно (по пятницам в 16:00); • Копирование обновлений – расписание отключено; • Откат обновления баз – расписание не предусмотрено; Во вновь созданных пользовательских задачах проверки по требованию расписание отключено.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 5.7.1 на стр. 60;
- в приложении Kaspersky Administration Kit, см. п. 21.3 на стр. 342.

A.2.2. Дата начала действия расписания и время запуска задачи

Параметр	Дата начала действия расписания и время запуска задачи.
Описание	Следующие параметры являются обязательными. • **Дата начала действия расписания (Начать с)**. Начиная с указанной вами даты, Антивирус будет запускать задачу с заданной расписанием частотой. • **Начать с** (применяется, если в качестве параметра **Частота** вы выбрали **Ежечасно**). Антивирус запустит задачу первый раз в указанное вами время. • **Время запуска** (применяется, если в качестве параметра **Частота запуска** вы выбрали **Ежедневно**, **Еженедельно**). Антивирус будет запускать задачу в указанное вами время с периодичностью, указанной параметром **Частота запуска**.
Возможные значения	Укажите дату и время.
Значение по умолчанию	Во вновь созданных пользовательских задачах проверки по требованию эти параметры выключены. В локальных системных задачах эти параметры по умолчанию имеют следующие значения: • Полная проверка компьютера – каждую пятницу в 20:00, в соответствии с настройками времени на защищаемом сервере; • Обновление баз приложения – каждые три часа. В расписании остальных системных задачах по умолчанию эти параметры выключены.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 5.7.1 на стр. 60;
- в приложении Kaspersky Administration Kit, см. п. 21.3 на стр. 342.

A.2.3. Дата окончания действия расписания

Параметр	Дата окончания действия расписания (**Отменить расписание с**).
Описание	Начиная с указанной вами даты расписание перестанет действовать: задача по расписанию запускаться не будет. Этот параметр не применяется, если качестве значения параметра расписания **Частота запуска** вы выбрали **При запуске приложения** или **После обновления баз**.
Возможные значения	Введите дату или выберите ее в диалоговом окне **Календарь**.
Значение по умолчанию	Не установлена

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 5.7.1 на стр. 60;
- в приложении Kaspersky Administration Kit, см. п. 21.3 на стр. 342.

A.2.4. Максимальная длительность выполнения задачи

Параметр	Максимальная длительность выполнения задачи.
Описание	Если задача будет выполняться дольше указанного вами количества часов и минут, она будет остановлена Антивирусом. Остановленная таким образом задача не будет считаться пропущенной. С помощью этого параметра вы также можете задавать время автоматической остановки задач постоянной защиты. Этот параметр не применяется в задачах обновления.
Возможные значения	Укажите количество часов и минут.
Значение по умолчанию	Выключен

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 5.7.1 на стр. 60;
- в приложении Kaspersky Administration Kit, см. п. 21.3 на стр. 342.

A.2.5. Промежуток времени в пределах суток, в течение которого задача будет приостановлена

Параметр	Промежуток времени в пределах суток, в течение которого задача будет приостановлена (**Приостановить с… до**).
Описание	Если требуется, вы можете приостановить задачу на указанный промежуток времени в пределах суток, например, приостановить задачу проверки по требованию, если нагрузка на сервер в это время суток высока и вы не хотите создавать дополнительную нагрузку за счет выполнения этой задачи. Этот параметр не применяется в задачах обновления. Если одновременно с этим параметром вы включили параметр **Максимальная длительность выполнения задачи**, обратите внимание, что указанный параметром промежуток времени, в течение которого задача будет приостановлена, входит в общую продолжительность выполнения задачи.
Возможные значения	Укажите промежуток времени в пределах суток.
Значение по умолчанию	Не указан.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 5.7.1 на стр. 60;
- в приложении Kaspersky Administration Kit, см. п. 21.3 на стр. 342.

A.2.6. Запуск пропущенных задач

Параметр	Запуск пропущенных задач.
Описание	Вы можете включить запуск пропущенных задач. Если Антивирус не сможет запустить задачу в заданное расписанием время (например, компьютер будет выключен), Антивирус признает эту задачу *пропущенной* и автоматически начнет ее выполнять, как только он будет снова запущен. Этот параметр не применяется, если в качестве параметра **Частота запуска** вы выбрали **При запуске приложения** или **После обновления баз**.
Возможные значения	Включен / выключен.
Значение по умолчанию	Выключен.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 5.7.1 на стр. 60;
- в приложении Kaspersky Administration Kit, см. п. 21.3 на стр. 342.

A.2.7. Распределение времени запуска в интервале, мин

Параметр	Распределение времени запуска в интервале, мин.
Описание	Если вы укажете значение этого параметра, то задача будет запускаться в произвольный момент в промежутке между расчетным временем ее запуска по расписанию и расчетным временем запуска плюс значение этого параметра. Вы можете применить этот параметр, например, когда вы используете один компьютер-посредник для распределения обновлений на многие серверы, чтобы снизить нагрузку на компьютер-посредник и сетевой трафик. Этот параметр не применяется, если вы выбрали тип запуска **При запуске приложения**, **После обновления баз** или **После получения обновлений Сервером администрирования**.
Возможные значения	Укажите количество минут.
Значение по умолчанию	Не задан.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 5.7.1 на стр. 60;
- в приложении Kaspersky Administration Kit, см. п. 21.3 на стр. 342.

A.3. Параметры безопасности в задаче *Постоянная защита файлов* и задачах проверки по требованию

В задаче **Постоянная защита файлов** и задачах проверки по требованию применяются следующие параметры безопасности:

- режим защиты объектов (только в задаче **Постоянная защита файлов**) (см. п. A.3.1 на стр. 399);
- проверяемые объекты (см. п. A.3.2 на стр. 400);
- проверка только новых и измененных объектов (см. п. A.3.3 на стр. 402);
- проверка составных объектов (см. п. A.3.4 на стр. 403);
- действие над зараженными объектами (см. п. A.3.5 на стр. 404);
- действие над подозрительными объектами (см. п. A.3.6 на стр. 407);
- действия над объектами в зависимости от типа угрозы (см. п. A.3.7 на стр. 409);
- исключение объектов (см. п. A.3.8 на стр. 411);
- исключение угроз (см. п. A.3.9 на стр. 412);
- максимальная продолжительность проверки объекта (см. п. A.3.10 на стр. 414);
- максимальный размер проверяемого составного объекта (см. п. A.3.11 на стр. 415);
- применение технологии iChecker (см. п. A.3.12 на стр. 416);
- применение технологии iSwift (см. п. A.3.13 на стр. 417).

A.3.1. Режим защиты объектов

Параметр безопасности **Режим защиты объектов** применяется только в задаче **Постоянная защита файлов**.

Параметр	Режим защиты объектов.
Описание	Этот параметр применяется только в задаче **Постоянная защита файлов**. Он определяет, при каком типе доступа к объектам Антивирус будет их проверять. Параметр **Режим защиты объектов** имеет единое значение для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.
Значения и некоторые рекомендации по их использованию	Выберите один из режимов защиты в зависимости от ваших требований к безопасности сервера, от того, файлы каких форматов хранятся на сервере и какую информацию они содержат: • **Интеллектуальный режим**. Антивирус проверяет объект при открытии и проверяет его повторно после сохранения, если объект был изменен. Если процесс во время своей работы многократно обращается к объекту и изменяет его, Антивирус повторно проверяет объект только после его последнего сохранения этим процессом. • **При открытии и изменении**. Антивирус проверяет объект при открытии и проверяет его повторно при сохранении, если объект был изменен. • **При открытии**. Антивирус проверяет объект при открытии как на чтение, так и на выполнение или изменение. • **При выполнении**. Антивирус проверяет объект только при открытии на выполнение. По умолчанию объекты проверяются в режиме защиты **При открытии и изменении**.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 6.2.3 на стр. 89;
- в приложении Kaspersky Administration Kit, см. п. 21.3 на стр. 342.

A.3.2. Проверяемые объекты

Параметр безопасности **Проверяемые объекты** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	Проверяемые объекты.
Описание	Этот параметр определяет, будут ли проверяться все объекты области защиты или только объекты с определенными форматами или расширениями. Вирусные аналитики «Лаборатории Касперского» составляют списки форматов и расширений, которые могут иметь объекты, подверженные заражению. Эти списки хранятся в базах Антивируса. Когда в «Лаборатории Касперского» они обновляются, вы получаете эти обновления вместе с обновлениями баз. С помощью параметра **Проверяемые объекты** вы можете сформировать свой список расширений.
Значения и некоторые рекомендации по их использованию	Выберите одно из следующих значений: • **Все объекты**. Антивирус проверяет любые объекты независимо от их расширения или формата; • **Объекты, проверяемые по формату**. Перед проверкой объекта Антивирус определяет его формат. Если формат объекта есть в списке форматов, свойственных заражаемым объектам, то Антивирус проверяет этот объект. Если формат объекта отсутствует в списке (например, текстовый файл не может быть заражен), Антивирус пропускает этот объект; • **Объекты, проверяемые по заданному списку расширений**. Антивирус проверяет только объекты, расширения которых входят в список расширений, свойственных заражаемым объектам. Если расширение объекта отсутствует в списке, Антивирус пропускает этот объект. Если вы выберете значение **Объекты, проверяемые по заданному списку расширений**, скорость проверки будет выше, чем в случае, если вы выберете значение **Объекты, проверяемые по формату**. Однако риск заражения будет выше, поскольку расширения объектов могут не соответствовать их формату. Например, если объекту присвоено расширение .txt, это не означает, что этот объект имеет текстовый формат. Объект может оказаться исполняемым файлом и содержать угрозу. Но Антивирус

	пропустит его, так как расширение .txt не входит в список расширений, свойственных заражаемым объектам. • **Объекты, проверяемые по указанным по маскам расширений**. Антивирус проверяет объекты с расширениями, которые есть в указанном вами списке (по умолчанию это список пуст). Вы можете добавлять в список новые расширения или маски расширений, а также удалять из него существующие. В масках расширений вы можете использовать символы: * и ?. Вы можете добавить все расширения из списка расширений, поставляемого с Антивирусом. Для этого в диалоговом окне редактирования списка нажмите на кнопку **По умолчанию**. **Загрузочные секторы дисков и MBR**. Этот параметр применяется, если в область проверки входят предопределенные области **Жесткие диски** и **Съемные диски**, предопределенная область **Мой компьютер** или динамически создаваемые диски. Этот параметр не применяется, если в область проверки входят только области **Системная память**, **Объекты автозапуска**, **Папки общего доступа**, а также если в область проверки входят отдельные файлы или папки. **Альтернативные потоки NTFS**. Антивирус проверяет дополнительные потоки файлов и папок на дисках файловой системы NTFS.

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.3. Проверка только новых и измененных объектов

Параметр безопасности **Проверка только новых и измененных объектов** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	**Проверка только новых и измененных объектов**.
Описание	Когда проверка только новых и измененных объектов включена, Антивирус проверяет все объекты указанной области защиты (проверки) кроме тех, которые он, проверив однажды, признал незараженными и которые не изменились с момента проверки.
Значения и некоторые рекомендации по их использованию	**Включить** / **Отключить**.

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.4. Проверка составных объектов

Параметр безопасности **Проверка составных объектов** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	Проверка составных объектов.
Описание	Проверка составных объектов занимает значительное время. По умолчанию Антивирус проверяет только составные объекты тех типов, которые наиболее подвержены заражению и которые наиболее опасны для сервера, если заражены. Составные объекты остальных типов не проверяются. Этот параметр позволяет вам, в соответствии с вашими требованиями к безопасности, выбирать типы составных объектов, которые Антивирус будет проверять.
Значения и некоторые рекомендации по их использованию	Выберите одно или несколько значений: • **Архивы**. Антивирус проверяет обычные архивы. Обратите внимание, что Антивирус обнаруживает угрозы в обычных архивах большинства типов, а лечит только архивы ZIP, ARJ, RAR и CAB; • **SFX-архивы**. Антивирус проверяет модуль-распаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive); • **Почтовые базы**. Антивирус проверяет файлы почтовых баз Microsoft Office Outlook и Microsoft Outlook Express; • **Упакованные объекты**. Антивирус проверяет исполняемые файлы, упакованные программами-упаковщиками двоичного кода, такими как UPX или ASPack. Составные объекты этого типа чаще других содержат в себе угрозы; • **Файлы почтовых форматов**. Антивирус проверяет файлы почтовых форматов, например, сообщения Microsoft Office Outlook или Microsoft Outlook Express; • **Вложенные OLE-объекты**. Антивирус проверяет объекты, вложенные в файлы документов Microsoft Office. Документы Microsoft Office часто включают исполняемые объекты, которые могут содержать угрозы. Если для выбранной области защиты (проверки) отключен параметр безопасности **Проверка только новых и измененных объектов**, то вы можете включать или выключать проверку только новых и измененных объектов индивиду-

	ально для каждого типа составных объектов. Если проверка только новых и измененных объектов включена, Антивирус проверяет все составные объекты указанной области защиты (проверки) кроме тех, которые он, проверив однажды, признал незараженными и которые не изменились с момента проверки.

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.5. Действие над зараженными объектами

Параметр безопасности **Действие над зараженными объектами** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

A.3.5.1. В задаче *Постоянная защита файлов*

Параметр	Действие над зараженными объектами.
Описание	Когда Антивирус признает проверяемый объект зараженным, он блокирует доступ к объекту для приложения, которое к нему обращается, и выполняет над объектом указанное вами действие. Перед изменением объекта (его лечением или удалением) Антивирус помещает копию объекта в резервное хранилище – специальную папку, в которой объекты хранятся в зашифрованном виде. Информацию о резервном хранилище содержит Глава 12 на стр. 189. Антивирус не пытается вылечить или удалить объект, если ему не удается предварительно сохранить его копию в резервном хранилище. Объект остается неизменным. Информация о том, почему Антивирусу не удалось вылечить или удалить объект, появляется в подробном отчете о выполнении задачи.

Значения параметра и некоторые рекомендации по их использованию	Выберите одно из следующих значений: • **Блокировать доступ + лечить**. Антивирус пытается вылечить объект, а если лечение невозможно, оставляет объект неизменным (объект недоступен для приложения, которое к нему обратилось); • **Блокировать доступ + лечить, удалять, если лечение невозможно**. Антивирус пытается вылечить объект, а если лечение невозможно, удаляет его; • **Блокировать доступ + удалять**. Антивирус удаляет зараженный объект; • **Блокировать доступ + выполнять рекомендуемое действие**. Антивирус автоматически подбирает и выполняет действия над объектом на основе данных об опасности обнаруженной в объекте угрозы и возможности его лечения; например, Антивирус сразу удаляет троянские программы, так как они не внедряются в другие файлы и не заражают их, и поэтому не предполагают лечения; • **Блокировать доступ**. Объект остается неизменным: Антивирус не пытается вылечить или удалить его, а только блокирует к нему доступ.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 6.2.2.2 на стр. 82;
- в приложении Kaspersky Administration Kit, см. П. 19.3 на стр. 290.

A.3.5.2. В задачах проверки по требованию

Параметр	Действие над зараженными объектами.
Описание	Когда Антивирус признает проверяемый объект зараженным, он выполняет над ним указанное вами действие. Перед изменением объекта (его лечением или удалениием) Антивирус помещает копию объекта в резервное хранилище – специальную папку, в которой объекты хранятся в зашифрованном виде. Информацию о резервном хранилище содержит Глава 12 на стр. 189; Антивирус не пытается вылечить или удалить объект, если ему не удается предварительно сохранить его копию в резервном хранилище. Объект остается неизменным. Информация о том, почему Антивирусу не удалось вылечить или удалить объект, регистрируется в подробном отчете о выполнении задачи.
Значения параметра и некоторые рекомендации по их использованию	Выберите одно из следующих значений: • **Лечить**. Антивирус пытается вылечить объект, а если лечение невозможно, оставляет объект неизменным; • **Лечить, удалять, если лечение невозможно**. Антивирус пытается вылечить объект, а если лечение невозможно, удаляет его; • **Удалять**. Антивирус сразу удаляет зараженный объект, не пытаясь его лечить; • **Выполнять рекомендуемое действие**. Антивирус автоматически подбирает и выполняет действия над объектом на основе данных об опасности обнаруженной в объекте угрозы и возможности лечения объекта; например, Антивирус сразу удаляет троянские программы, так как они не внедряются в другие файлы и не заражают их, и поэтому не предполагают лечения; • **Пропускать**. Объект остается неизменным, Антивирус не пытается вылечить или удалить его. Информация об обнаруженном зараженном объекте сохраняется в подробном отчете о выполнении задачи.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.6. Действие над подозрительными объектами

Параметр безопасности **Действия над подозрительными объектами** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

A.3.6.1. В задаче *Постоянная защита файлов*

Параметр	Действие над подозрительными объектами.
Описание	Когда Антивирус признает проверяемый объект подозрительным, он блокирует доступ к объекту для приложения, которое к нему обращается, и выполняет над объектом указанное вами действие. Перед удалением объекта Антивирус помещает его копию в резервное хранилище – специальную папку, в которой объект хранится в зашифрованном виде. Информацию о резервном хранилище содержит Глава 12 на стр. 189.
Значения и некоторые рекомендации по их использованию	Выберите одно из следующих значений: • **Блокировать доступ + помещать на карантин**. Объект переносится в специальную папку (карантин), в которой он хранится в зашифрованном виде. Информацию о пользовании карантином содержит Глава 11 на стр. 169; • **Блокировать доступ + удалять**. Антивирус удаляет подозрительный объект с диска; Антивирус не удаляет объект, если ему не удается предварительно поместить его копию на карантин. Объект остается неизменным. Информация о том, почему Антивирусу не удалось удалить объект, появляется в подробном отчете о выполнении задачи. • **Блокировать доступ + выполнять рекомендуемое действие**. Антивирус подбирает и выполняет действия над объектом на основе данных о том, насколько опасна обнаруженная в объекте угроза; • **Блокировать доступ**. Объект остается неизменным: Антивирус не пытается вылечить или удалить его, а только блокирует к нему доступ.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 6.2.2.2 на стр. 82;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.6.2. В задачах проверки по требованию

Параметр	Действие над подозрительными объектами.
Описание	Когда Антивирус признает проверяемый объект подозрительным, он выполняет над ним указанное вами действие. Перед удалением объекта Антивирус помещает его копию в резервное хранилище – специальную папку, в которой объект хранится в зашифрованном виде. Информацию об использовании резервного хранилища содержит Глава 12 на стр. 189.
Значения и некоторые рекомендации по их использованию	Выберите одно из следующих значений: • **Помещать на карантин**. Объект переносится в специальную папку (карантин), в которой он хранится в зашифрованном виде. Информацию о пользовании карантином содержит Глава 11 на стр. 169; • **Удалять**. Антивирус удаляет подозрительный объект с диска; Антивирус не удаляет объект, если ему не удается предварительно поместить его копию на карантин. Объект остается неизменным. Информация о том, почему Антивирусу не удалось удалить объект, появляется в подробном отчете о выполнении задачи. • **Выполнять рекомендуемое действие**. Антивирус подбирает и выполняет действия над объектом на основе данных о том, насколько опасна обнаруженная в объекте угроза; • **Пропускать**. Объект остается неизменным: Антивирус не пытается вылечить или удалить его. Информация об обнаруженном подозрительном объекте сохраняется в подробном отчете о выполнении задачи.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.7. Действия в зависимости от типа угрозы

Параметр безопасности **Действия в зависимости от типа угрозы** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	Действия в зависимости от типа угрозы (**Выполнять действие согласно типу угроз**).
Описание	Угрозы некоторых типов представляют для сервера большую опасность, чем другие. Например, троянская программа может нанести гораздо более серьезный урон, чем программа-реклама. С помощью параметров этой группы вы можете настроить различные действия Антивируса над объектами, которые содержат угрозы разных типов. Если вы установите значения этого параметра, то Антивирус применит их вместо значений параметров **Действие над зараженными объектами** и **Действие над подозрительными объектами**.
Значения и некоторые рекомендации по их использованию	Для каждого типа угроз выберите в списке возможных действий над зараженными и подозрительными объектами два действия, которые Антивирус попытается выполнить над объектом, если он обнаружит в нем угрозу указанного типа. Антивирус выполнит второе действие над объектом, если ему не удастся выполнить первое действие. Антивирус будет применять указанные действия как к зараженным, так и к подозрительным объектам, если это возможно. К примеру, если вы выберете первое действие **Лечить**, а второе – **Помещать на карантин**, Антивирус поместит зараженный объект на карантин, только если ему не удастся его вылечить, и поместит подозрительный объект на карантин сразу, пропустив действие **Лечить**, поскольку подозрительные объекты не подлежат лечению. Если вы выберете **Пропускать** в качестве первого действия, то второе действие будет недоступно. Для остальных значений рекомендуется указать два действия. Обратите внимание, что в списке типов угроз типы *Сетевые черви* и *Классические вирусы объединены* под одним названием *Вирусы*. Если Антивирусу не удается поместить объект в резервное

	хранилище или на карантин, то он не выполняет последующее действие над объектом (например, его лечение или удаление). Объект считается пропущенным. Вы можете просмотреть причину пропуска объекта в подробном отчете о выполнении задачи. В списке типов угроз значение **Не определено** включает новые вирусы, на текущий момент не причисленные ни к одному из известных типов. Типы угроз описаны в п. 1.1.2 на стр. 16.
Значение по умолчанию	Выключен

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.8. Исключение объектов

Параметр безопасности **Исключение объектов** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	Исключение объектов (**Исключать объекты**).
Описание	С помощью этого параметра вы можете исключать из проверки отдельные файлы или сразу несколько файлов по маске имени файла. Исключив из проверки файлы большого размера, вы можете ускорить файловый обмен и снизить время выполнения задач проверки по требованию. Информация о том, что объект исключен из проверки, заносится в подробный отчет о выполнении задачи (в соответствии с параметрами отчетов, установленными по умолчанию). Подробнее об отчетах читайте в п. 13.2 на стр. 204. В задачах проверки по требованию, когда Антивирус будет проверять процесс в памяти, он проверит и запускающий файл процесса, даже если этот файл добавлен в список исключений.
Значения и некоторые рекомендации по их использованию	Сформируйте список файлов. Вы можете указать имя файла как полностью, так и с помощью маски. Для задания масок используйте специальные символы * и ?.
Значение по умаолчанию	Список пуст.

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.9. Исключение угроз

Параметр безопасности **Исключение угроз** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	Исключение угроз (**Исключать угрозы**).
Описание	Если Антивирус признает проверяемый объект зараженным или подозрительным и выполняет действия над ним, а вы считаете этот объект безопасным для защищаемого сервера, вы можете исключить угрозу, обнаруженную в объекте, из списка угроз, которые Антивирус обрабатывает. Вы можете исключить одну угрозу по ее имени в конкретном объекте или целый тип угроз. Если вы исключите угрозу, Антивирус признает объекты, которые содержат эту угрозу, незараженными.
Значения и некоторые рекомендации по их использованию	Сформируйте список исключаемых угроз (по умолчанию этот список пуст). Разделяйте значения в списке точкой с запятой (;). Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Антивируса о том, что объект является зараженным или подозрительным. Полное название угрозы определяется в результате проверки объекта. Оно может содержать следующую информацию: **<класс угрозы>:<тип угрозы>.<краткое название платформы>.<имя угрозы>.<код модификации угрозы>**. Например, вы используете утилиту Remote Administrator в качестве средства удаленного управления. Большинство антивирусных приложений относят код этой утилиты к угрозам типа *Потенциально опасные программы*. Чтобы Антивирус не блокировал ее, добавьте полное название угрозы в ней в список исключаемых угроз того узла в дереве файловых ресурсов сервера, в котором хранятся файлы утилиты. В качестве значения параметра вы можете указать: • полное название угрозы: **not-a-virus:RemoteAdmin.Win32.RAdmin.20**. Антивирус не будет выполнять действий только над модулями программы, в которой Антивирус обнаружит угрозу с названием Win32.RAdmin.20. • маску полного названия угрозы: **not-virus:RemoteAdmin.***

	Антивирус не будет выполнять действий над программами Remote Administrator всех версий. • маску полного названия угрозы, включающую только тип угрозы: **not-a-virus:*** Антивирус не будет выполнять никаких действий над всеми объектами, в которых присутствует угроза этого типа. Вы можете найти полное название угрозы, обнаруженной в программном продукте, в подробном отчете о выполнении задачи. Подробнее об отчетах читайте в п. 13.2 на стр. 204. Вы также можете найти полное название угрозы, обнаруженной в объекте, на веб-сайте Вирусной энциклопедии Viruslist.ru. Чтобы найти название угрозы, введите название программного продукта в поле **Поиск**.

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.10. Максимальная продолжительность проверки объекта

Параметр безопасности **Максимальная продолжительность проверки объекта** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	Максимальная продолжительность проверки объекта, сек (**Останавливать проверку, если она длится более … сек.**).
Описание	Антивирус прекращает проверку объекта, если она длится дольше указанного значением параметра количества секунд. Информация о том, что объект исключен из проверки, заносится в подробный отчет о выполнении задачи (в соответствии с параметрами отчетов, установленными по умолчанию).
Значения	Введите максимальную продолжительность проверки объекта в секундах.

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.11. Максимальный размер проверяемого составного объекта

Параметр безопасности **Максимальный размер проверяемого составного объекта** применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	Максимальный размер проверяемого составного объекта, МБ (**Не проверять составные объекты размером более … МБ**).
Описание	Если размер проверяемого составного объекта превышает указанное значение, Антивирус пропускает объект. Информация о том, что объект пропущен, заносится в подробный отчет о выполнении задачи (в соответствии с параметрами отчетов, установленными по умолчанию).
Значения	Задайте максимальный размер составного объекта в мегабайтах.

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.12. Применение технологии iChecker

Параметр безопасности Применение технологии iChecker используется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	Применение технологии iChecker (**Использовать технологию iChecker**).
Описание	Этот параметр включает или выключает применение технологии iChecker, разработанной в «Лаборатории Касперского». Технология iChecker применяется только к объектам типов и форматов, свойственных объектам, подверженным заражению. Технология iChecker позволяет не проверять повторно объекты на сервере, которые в результате предыдущих проверок были признаны Антивирусом незараженными. Использование iChecker снижает нагрузку на процессор и дисковые системы и еще более повышает скорость проверки и ускоряет файловый обмен. Обратите внимание, что Антивирус проверяет объект повторно, если за время, истекшее с предыдущей проверки, изменился сам объект или изменились параметры безопасности в сторону повышения уровня безопасности. Антивирус заносит в отчет информацию о том, что объект не проверен в результате применения технологии iChecker (в соответствии с параметрами отчетов, установленными по умолчанию).
Значения	Включено / выключено.

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.3.13. Применение технологии iSwift

Параметр безопасности Применение технологии iSwift применяется в задаче **Постоянная защита файлов** и задачах проверки по требованию.

Параметр	Применение технологии iSwift (**Использовать технологию iSwift**).
Описание	Этот параметр включает или выключает применение технологии iSwift, разработанной в «Лаборатории Касперского». Технология iSwift применяется к объектам файловой системы NTFS. Технология iSwift позволяет не проверять повторно объекты, которые в результате предыдущих проверок были признаны Антивирусом незараженными, а также объекты, проверенные другими антивирусными приложениями «Лаборатории Касперского» версии 6.0. Использование iSwift снижает нагрузку на процессор и дисковые системы и еще более повышает скорость проверки и ускоряет файловый обмен. Обратите внимание, что Антивирус проверяет объект повторно, если за время, истекшее с предыдущей проверки, изменился сам объект или изменились параметры безопасности в сторону повышения уровня безопасности. Антивирус заносит в отчет информацию о том, объект не проверен в результате применения технологии iSwift (в соответствии с параметрами отчетов, установленными по умолчанию). В Антивирусе используется iNetSwift – сетевая версия технологии iSwift. Она работает так же, как и обычная, но позволяет не проверять повторно файлы, полученные с других компьютеров в сети, на которых установлено одно из следующих приложений и работает iSwift. • Kaspersky Anti-Virus 6.0 for Windows Workstations; • Kaspersky Anti-Virus 6.0 for Windows Servers; • Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition; • Kaspersky Anti-Virus 6.0 / 7.0; • Kaspersky Internet Security 6.0 / 7.0. Применение iNetSwift исключает повторную обработку объектов в рамках сети, сводя к минимуму влияние Антивируса

	на скорость файлового обмена. Если на защищаемом сервере установлен Novell Client For Windows XP/2003 версии 4.71 или выше, технология iSwift работает только в рамках одного компьютера, не используя iNetSwift.
Значения	Включено / выключено.

О том, как настроить параметр:

- в консоли Антивируса в MMC, в задаче **Постоянная защита файлов** – см. п. 6.2.2.2 на стр. 82; в задаче проверки по требованию – см. п. 9.2.2.2 на стр. 135;
- в приложении Kaspersky Administration Kit, см. п. 19.3 на стр. 290.

A.4. Параметры автоматического блокирования доступа с компьютеров к серверу

В этом приложении описаны следующие параметры автоматического блокирования доступа с компьютеров к серверу:

- включение / выключение автоматического блокирования доступа с компьютеров (см. п. A.4.1 на стр. 419);
- действия над зараженными компьютерами (см. п. A.4.2 на стр. 420);
- список компьютеров, исключенных из блокирования (см. п. A.4.3 на стр. 421);
- предотвращение вирусных эпидемий (см. п. A.4.4 на стр. 422).

A.4.1. Включение / выключение блокирования доступа с компьютеров к серверу

Параметр	Включение / выключение блокирования доступа с компьютеров к серверу.
Описание	Этот параметр включает или выключает автоматическое блокирование доступа с компьютеров при попытке записи на сервер зараженного или подозрительного файла. Антивирус не выполняет автоматическое блокирование доступа с компьютеров, если в задаче **Постоянная защита файлов** в качестве значения параметра **Режим защиты объектов** выбрано значение **При открытии** или **При выполнении**. В этом случае вы можете заблокировать доступ с зараженного компьютера вручную. Если вы включите блокирование доступа с компьютеров к серверу, оно будет выполняться только тогда, когда выполняется задача **Постоянная защита файлов**.
Возможные значения	Включить / выключить.
Значение по умолчанию	Выключен.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 7.2 на стр. 97;
- в приложении Kaspersky Administration Kit, см. п. 20.3.1 на стр. 304.

A.4.2. Действия над зараженными компьютерами

Параметр	Действия над зараженными компьютерами.
Описание	Если автоматическое блокирование включено, как только какой-либо компьютер в локальной сети попытается записать на защищаемый сервер зараженный или подозрительный объект, Антивирус выполнит указанные вами действия. Вы можете указать одно или два действия: • **Блокировать доступ с компьютера к серверу**. Антивирус заблокирует доступ с компьютера к серверу на указанный промежуток времени; • **Запускать исполняемый файл**. Антивирус запустит на сервере указанный исполняемый файл. Инструкции в исполняемом файле могут определять действия, которые выполнит не Антивирус, а другое указанное приложение. Например, исполняемый файл может содержать командную строку, выполнение которой добавит зараженный компьютер в настройки сетевого экрана. Вы можете включить имя зараженного компьютера в текст исполняемого файла с помощью специального параметра командной строки Антивируса: %COMPUTER_NAME%. При выборе исполняемого файла вы можете также добавлять ключи командной строки, которые поддерживает приложение, запускаемое из этого файла.
Возможные значения	Если вы выбрали **Блокировать доступ с компьютера к серверу**, то задайте промежуток времени, на который вы хотите заблокировать доступ к серверу с зараженных компьютеров, в днях, часах или минутах. Если вы выбрали **Запускать исполняемый файл**, укажите имя исполняемого файла и полный путь к нему и укажите учетную запись, с правами которой исполняемый файл будет выполнен. Исполняемый файл должен храниться на локальном диске защищаемого сервера. Учетная запись, с правами которой будет выполнен файл, должна быть зарегистрирована на защищаемом сервере или контроллере домена, в который входит защищаемый сервер.
Значение по умолчанию	Блокирование на 15 минут.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 7.3 на стр. 98;
- в приложении Kaspersky Administration Kit, см. п. 20.3.2 на стр. 305.

A.4.3. Список доверенных компьютеров

Параметр	Список доверенных компьютеров.
Описание	Вы можете задать список компьютеров, исключенных из автоматического блокирования, – компьютеров локальной сети, над которыми Антивирус не выполнит никаких действий, если произойдет попытка записи с такого компьютера на защищаемый сервер зараженного или подозрительного объекта. Если вы добавите в список компьютер, доступ с которого в текущий момент заблокирован, то он не будет разблокирован сразу после того, как вы сохраните новые параметры блокирования. Он будет разблокирован только после того, как истечет заданный промежуток времени его блокирования или вы разблокируете его вручную.
Возможные значения	Сформируйте список компьютеров, исключенных из блокирования, указав для каждого компьютера его сетевое имя, IP-адрес или диапазон IP-адресов. Вы можете указывать только сетевые NetBIOS-имена компьютеров, вы не можете указывать DNS-имена.
Значение по умолчанию	Список пуст.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 7.4 на стр. 100;
- в приложении Kaspersky Administration Kit, см. п. 20.3.3 на стр. 307.

A.4.4. Предотвращение вирусных эпидемий

Параметр	Предотвращение вирусных эпидемий.
Описание	Если функция *Предотвращение вирусных эпидемий* включена, Антивирус повышает уровень защиты в выполняющейся задаче **Постоянная защита файлов**, как только количество компьютеров с заблокированным доступом к серверу достигает указанного значения. Антивирус применяет ко всей области защиты единые параметры безопасности, описанные в таблице 30. Если включено восстановление уровня безопасности, то, когда количество компьютеров с заблокированным доступом снижается до указанного значения, Антивирус возвращается к использованию значений параметров безопасности, указанных в задаче **Постоянная защита файлов**. Если вы измените значения параметров безопасности, описанные в таблице 30, в выполняющейся задаче **Постоянная защита файлов** после автоматического повышения уровня безопасности и до его восстановления, то новые значения параметров применятся не сразу, а только когда Антивирус восстановит уровень безопасности или вы отключите предотвращение вирусных эпидемий. Информация об изменении параметров безопасности заносится в журнал системного аудита. Предотвращение вирусных эпидемий не применяется, если значения параметров безопасности в задаче **Постоянная защита файлов** определяются политикой приложения Kaspersky Administration Kit.
Возможные значения	Вы можете установить следующие значения: • Включить / выключить функцию *Предотвращение вирусных эпидемий*; указать количество заблокированных компьютеров, по достижению которого Антивирус повысит уровень безопасности; • Включить / выключить восстановление уровня безопасности, указать количество компьютеров, по достижению которого Антивирус восстановит уровень безопасности.
Значение по	Выключено.

умолчанию	Если вы включите функцию *Предотвращение вирусных эпидемий*, то по умолчанию применятся следующие значения: • Порог повышения уровня безопасности – 25 компьютеров; • Порог восстановления уровня безопасности – 15 компьютеров.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 7.5 на стр. 101;
- в приложении Kaspersky Administration Kit, см. п. 20.3.4 на стр. 308.

В следующей таблице приводятся значения параметров безопасности, которые применятся в задаче **Постоянная защита файлов**, когда количество компьютеров с заблокированным доступом к серверу достигнет указанного значения.

Таблица 30. Значения параметров безопасности функции *Предотвращение вирусных эпидемий*

Параметр безопасности	Значение
Режим защиты объектов (см. п. A.3.1 на стр. 399)	При открытии и изменении
Проверяемые объекты (см. п. A.3.2 на стр. 400)	По формату
Проверка только новых и измененных объектов (см. п. A.3.3 на стр. 402)	Выключена
Действие над зараженными объектами (см. п. A.3.5 на стр. 404)	Лечить; удалять, если лечение невозможно
Действие над подозрительными объектами (см. п. A.3.6 на стр. 407)	Помещать на карантин

Параметр безопасности	Значение
Проверка составных объектов (см. п. A.3.4 на стр. 403)	Включаются следующие значения параметра: • все SFX-архивы; • все упакованные объекты; • все вложенные OLE-объекты. Остаются неизменными следующие значения параметра: • архивы; • почтовые базы; • файлы почтовых форматов.
Проверка дополнительных потоков файловой системы (NTFS) (см. п. A.3.2 на стр. 400)	Включена
Проверка загрузочных секторов дисков и MBR (см. п. A.3.2 на стр. 400)	Включена
Максимальная продолжительность проверки объекта (см. п. A.3.10 на стр. 414);	60 сек.
Максимальный размер проверяемого составного объекта (см. п. A.3.11 на стр. 415);	Не установлен

Не изменяются значения следующих параметров безопасности:

- Исключение объектов (см. п. A.3.8 на стр. 411);
- Исключение угроз (см. п. A.3.9 на стр. 412);
- Применение технологии iChecker (см. п. A.3.12 на стр. 416);
- Применение технологии iSwift (см. п. A.3.13 на стр. 417).

A.5. Параметры задач обновления

В задачах обновления Антивирус применяет следующие параметры:

- параметры, общие для всех задач обновления:
  - источник обновлений (см. п. A.5.1 на стр. 426);
  - режим FTP-сервера для соединения с защищаемым сервером (см. п. A.5.2 на стр. 427);
  - время ожидания при соединении с FTP-сервером (см. п. A.5.3 на стр. 428);
  - параметры прокси-сервера:
    - обращение к прокси-серверу при подключении к различным источникам обновлений (см. п. A.5.4.1 на стр. 429);
    - адрес прокси-сервера (см. п. A.5.4.2 на стр. 430);
    - метод проверки подлинности при доступе к прокси-серверу (см. п. A.5.4.3 на стр. 431);
  - региональные настройки для оптимизации получения обновлений (см. п. A.5.5 на стр. 432);
- параметры задачи **Обновление модулей приложения**:
  - копирование и установка обновлений модулей приложения или только проверка наличия (см. п. A.5.6.1 на стр. 433);
  - получение информации о выходе плановых обновлений модулей Антивируса (см. п. A.5.6.2 на стр. 434);
- параметры задачи **Копирование обновлений**:
  - состав обновлений (см. п. A.5.7.1 на стр. 435);
  - папка для сохранения обновлений (см. п. A.5.7.2 на стр. 437).

A.5.1. Источник обновлений

Параметр	Источник обновлений.
Описание	Вы можете выбрать источник, из которого Антивирус будет получать обновления баз или программных модулей, в зависимости от схемы обновления, используемой в вашей организации (примерные схемы обновления приводятся в п. 10.3 на стр. 152).
Возможные значения	В качестве источника обновлений вы можете указывать: • **Серверы обновлений «Лаборатории Касперского»**. Антивирус загрузит обновления с одного из серверов обновлений «Лаборатории Касперского», расположенных в различных географических точках. Обновления загружаются по протоколу HTTP или FTP. • **Сервер администрирования Kaspersky Administration Kit**. Вы можете выбрать этот источник обновления, если вы используете приложение Kaspersky Administration Kit для централизованного управления антивирусной защитой компьютеров в вашей организации. Антивирус будет копировать обновления на защищаемый сервер с установленного в локальной сети сервера администрирования Kaspersky Administration Kit. • **Другие HTTP-, FTP-серверы или сетевые ресурсы**. Антивирус будет копировать обновления из указанного вами источника: папки FTP- или HTTP-сервера или любого компьютера в локальной сети. Вы можете указать один или несколько пользовательских источников обновлений. Антивирус будет обращаться к каждому следующему указанному источнику, если предыдущий окажется недоступным. Вы можете задавать порядок обращения Антивируса к источникам, включать или отключать использование отдельных источников. Вы можете настроить обращение Антивируса к серверам обновлений «Лаборатории Касперского» в случае, если все пользовательские источники будут недоступны. **Примечание** Указывая пути, вы можете использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, укажите учетную запись этого пользователя для запуска задачи (см. п. 5.9 на стр. 64).

	Вы не можете выбирать в качестве источников обновлений папки на подключенных сетевых дисках.
Значение по умолчанию	Вы можете просмотреть список серверов обновлений «Лаборатории Касперского» в файле %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Update\updcfg.xml.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.1 на стр. 158;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.2. Режим FTP-сервера для соединения с защищаемым сервером

Параметр	Режим FTP-сервера для соединения с защищаемым сервером (**Использовать пассивный режим FTP, если возможно**).
Описание	Для соединения с серверами обновлений по протоколу FTP Антивирус использует пассивный режим FTP-сервера: предполагается, что в локальной сети организации используется сетевой экран. Когда пассивный режим FTP-сервера не работает, автоматически включается активный.
Возможные значения	Выберите режим FTP-сервера: включите или отключите использование пассивного режима FTP.
Значение по умолчанию	Пассивный режим FTP, если возможно.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.1 на стр. 158;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.3. Время ожидания при соединении источником обновлений

Параметр	Время ожидания при соединении (**Тайм-аут**).
Описание	Этот параметр задает время ожидания при соединении с источником обновлений.
Возможные значения	Укажите время ожидания в секундах.
Значение по умолчанию	10 сек.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.1 на стр. 158;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.4. Использование и параметры прокси-сервера

Антивирус применяет следующие параметры доступа к прокси-серверу:

- обращение к прокси-серверу при подключении к различным источникам обновлений (см. п. A.5.4.1 на стр. 429);
- параметры прокси-сервера (см. п. A.5.4.2 на стр. 430);
- метод проверки подлинности при доступе к прокси-серверу (см. п. A.5.4.3 на стр. 431).

A.5.4.1. Обращение к прокси-серверу при подключении к источникам обновлений

Параметр	Обращение к прокси-серверу при подключении к источникам обновлений.
Описание	По умолчанию при подключении к серверам обновлений «Лаборатории Касперского» Антивирус обращается к прокси-серверу в сети, а при подключении пользовательскими источниками обновлений (как к HTTP- или FTP-серверам, так и к указанным компьютерам), – он обходит прокси-сервер: предполагается, что эти источники находятся в локальной сети. Обратите внимание, что расширения файлов обновлений баз формируются случайным образом. Если на прокси-сервере в вашей сети установлен запрет на загрузку файлов с определенными расширениями, то рекомендуется разрешить загрузку файлов со всеми расширениями с серверов обновлений «Лаборатории Касперского». Вы можете просмотреть список серверов обновлений «Лаборатории Касперского» в файле %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Update\updcfg.xml.
Возможные значения	• Если в качестве источника обновлений вы указали сервера обновлений «Лаборатории Касперского», то убедитесь, что флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений «Лаборатории Касперского»** установлен.

	• Если для соединения с каким-либо из пользовательских FTP- или HTTP-серверов требуется доступ к прокси-серверу, установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**. Установив этот флажок, вы можете отключить обращение к прокси-серверу для доступа к остальным источникам обновления – тем, для которых обращение к прокси не требуется (например, компьютерам локальной сети): установите флажок **Не использовать прокси-сервер для локальных адресов**.
Значение по умолчанию	Антивирус обращается к прокси-серверу только при подключении к HTTP- или FTP-серверам обновлений «Лаборатории Касперского».

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.1 на стр. 158;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.4.2. Параметры прокси-сервера

Параметр	Параметры прокси-сервера.
Описание	При подключении к FTP- или HTTP-серверам обновлений Антивирус по умолчанию автоматически распознает параметры прокси-сервера, который используется в локальной сети, по протоколу Web Proxy Auto-Discovery Protocol (WPAD). Вы можете вручную указать параметры прокси-сервера, например, если протокол WPAD не настроен в вашей локальной сети.
Возможные значения	Укажите IP-адрес или DNS-имя сервера (например, proxy.mycompany.com) и его порт. Отключите использование прокси-сервера, если пользовательский FTP- или HTTP-сервер находится в вашей локальной сети.
Значение по умолчанию	Автоматически распознавать параметры прокси-сервера.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.1 на стр. 158;

- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.4.3. Метод проверки подлинности при доступе к прокси-серверу

Параметр	Метод проверки подлинности при доступе к прокси-серверу.
Описание	Этот параметр указывает метод проверки подлинности пользователя при доступе к прокси-серверу, который используется при соединении с FTP- или HTTP-серверами-источниками обновлений.
Возможные значения	Выберите одно из следующих значений: • **Не использовать аутентификацию**. Выберите, если для доступа к прокси-серверу не требуется проверка подлинности. • **Использовать NTLM-аутентификацию**. Антивирус будет использовать для доступа к прокси-серверу учетную запись, указанную в задаче. (Если параметром задачи **Запустить как** не указана другая учетная запись, то задача выполнится под учетной записью **Локальная система** (**SYSTEM**). Вы можете выбрать этот метод, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows (NTLM authentication) (об использовании учетных записей для запуска задач читайте в п. 5.9.1 на стр. 64). • **Использовать NTLM-аутентификацию с именем и паролем**. Антивирус будет использовать для доступа к прокси-серверу учетную запись, указанную вами. Вы можете выбрать этот метод, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows. Введите логин и пароль пользователя или выберите пользователя в списке. • **Использовать имя и пароль пользователя**. Вы можете выбрать обычную проверку подлинности (Basic authentication). Введите имя и пароль пользователя или выберите пользователя в списке. Вы можете выбрать этот метод, например, если учетная запись, с правами которой будет выполняться задача обновления, не имеет прав доступа к прокси-серверу и вы хотите использовать другую учетную запись.

	Если обычная проверка подлинности по имени и паролю пользователя не прошла, Антивирус выполняет встроенную проверку подлинности Microsoft Windows по учетной записи, используемой в задаче.
Значение по умолчанию	Проверка подлинности при доступе к прокси-серверу не выполняется.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.1 на стр. 158;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.5. Региональные настройки для оптимизации получения обновлений (Расположение защищаемого сервера)

Параметр	Региональные настройки для оптимизации получения обновлений (**Расположение**).
Описание	Серверы обновлений «Лаборатории Касперского» размещены в различных географических точках. С помощью этого параметра вы можете указать страну местоположения защищаемого сервера. Антивирус оптимизирует загрузку обновлений на защищаемый сервер с серверов обновлений «Лаборатории Касперского», выбрав ближайший к нему сервер обновлений.
Возможные значения	Вы можете выбрать страну местоположения защищаемого сервера.
Значение по умолчанию	По умолчанию Антивирус распознает местоположение защищаемого сервера в соответствии с региональными настройками Microsoft Windows, для Microsoft Windows Server 2003 – по значению переменной **Расположение** (**Location**), установленной для стандартного профиля пользователя (Default User Account Settings). Например, если в региональных настройках Microsoft Windows вы установите (под текущей учетной записью) переменную **Расположение** в значение **Россия**, тогда как для

	стандартного профиля пользователя она сохранится в значении **США**, Антивирус будет обращаться к серверам обновлений, установленным не на территории России, а на территории Соединенных Штатов Америки. Чтобы оптимизировать получение обновлений, вы можете выполнить одно из следующих действий: • в региональных настройках Microsoft Windows указать страну местоположения сервера переменной **Расположение**, применив значение переменной для стандартного профиля пользователя; • в Антивирусе запустить задачу обновления под текущей учетной записью; • выбрать страну местоположения сервера с помощью параметра обновления **Расположение защищаемого сервера**, описанного в этой таблице.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.1 на стр. 158;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.6. Параметры задачи *Обновление модулей приложения*

В задаче **Обновление модулей приложения** применяются следующие параметры:

- копирование и установка критических обновлений модулей приложения или только проверка их наличия (см. п. A.5.6.1 на стр. 433);
- получение информации о выходе плановых обновлений модулей Антивируса (см. п. A.5.6.2 на стр. 434).

A.5.6.1. Копирование и установка критических обновлений или только проверка их наличия

Параметр	Копирование и установка критических обновлений или только проверка их наличия.

Описание	С помощью параметров задачи **Обновление модулей приложения** вы можете выбрать, сразу загружать и устанавливать критические обновления программных модулей или только проверять их наличие.
Возможные значения	Выберите одно из следующих значений: • **Только проверять наличие доступных критических обновлений модулей приложения**. Вы можете выбрать этот вариант, например, для того, чтобы узнать о выпуске критических обновлений модулей Антивируса. • **Копировать и устанавливать доступные критические обновления модулей приложения**.
Значение по умолчанию	**Только проверять наличие доступных критических обновлений модулей приложения**.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.2 на стр. 163;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.6.2. Получение информации о выходе плановых обновлений модулей Антивируса

Параметр	Получение информации о доступных плановых обновлениях модулей Антивируса.
Описание	Вы можете получать информацию о доступных плановых обновлениях модулей Антивируса. Чтобы получать уведомления о выходе плановых обновлений, установите значение **Получать информацию о доступных плановых обновлениях модулей Антивируса** и настройте уведомление о событии Антивируса «Доступны обновления программных модулей», в котором будет содержаться адрес страницы нашего сайта, откуда вы сможете загрузить плановые обновления (подробнее о настройке уведомлений читайте в п. 15.2 на стр. 237).
Возможные значения	Получать / не получать информацию о доступных плановых обновлениях модулей Антивируса.

Значение по умолчанию	**Получить информацию о доступных плановых обновлениях моделй Антивируса**.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.2 на стр. 163;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.7. Параметры задачи *Копирование обновлений*

В задаче **Копирование обновлений** Антивирус применяет следующие параметры:

- состав обновлений в задаче **Копирование обновлений** (см. п. A.5.7.1 на стр. 435);
- папка для сохранения обновлений (см. п. A.5.7.2 на стр. 437).

A.5.7.1. Состав обновлений

Параметр	Состав обновлений.
Описание	С помощью этого параметра вы можете выбрать состав копируемых обновлений. Вы можете копировать только обновления баз Антивируса, только срочные обновления его программных модулей, все доступные обновления. Или вы можете копировать обновления баз и модулей не только Антивируса, но и остальных приложений «Лаборатории Касперского» версии 6.0, чтобы затем распределять эти обновления на другие компьютеры локальной сети, на которых установлены антивирусные приложения «Лаборатории Касперского» этой версии. По умолчанию Антивирус сохраняет файлы обновлений в папке %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\UpdateDistribution\.
Возможные значения	Выберите одно из следующих значений: • чтобы загружать и сохранять в указанную папку только обновления баз, выберите **Копировать обновления баз**

	приложения; • чтобы загружать и сохранять в указанную папку только обновления программных модулей, выберите **Копировать критические обновления модулей приложения**; • чтобы загружать и сохранять в указанную папку и обновления баз и обновления программных модулей, выберите **Копировать обновления баз и критические обновления модулей приложения**. Чтобы получать обновления баз и программных модулей не только для Антивируса, но и для остальных приложений «Лаборатории Касперского» версии 6.0 и выше, выберите **Копировать обновления баз и модулей для всех приложений «Лаборатории Касперского» версии 6.0 и выше**.
Значение по умолчанию	Антивирус копирует только обновления баз Антивируса.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.3 на стр. 165;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.5.7.2. Папка для сохранения обновлений

Параметр	Папка для сохранения обновлений.
Описание	С помощью этого параметра вы можете указать папку, в которой будут сохранены файлы обновлений.
Возможные значения	Укажите локальную или сетевую папку, в которую Антивирус сохранит скопированные обновления. Чтобы указать сетевую папку, введите ее имя и путь к ней в формате UNC (Universal Naming Convention). Вы не можете указывать папки на подключенных сетевых дисках, а также дисках, созданных с помощью команды SUBST. Указывая пути, вы можете использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, укажите учетную запись этого пользователя для запуска задачи (см. п. 5.9 на стр. 64). Если вы управляете Антивирусом на защищаемом сервере через консоль MMC, установленную на удаленном рабочем месте администратора, то вы должны входить в группу локальных администраторов на защищаемом сервере, чтобы просматривать папки на нем.
Значение по умолчанию	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Update\Distribution\ Вы можете использовать переменную окружения Антивируса %KAVWSEEAPPDATA%, чтобы указать папку Антивируса %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 10.5.3 на стр. 165;
- в приложении Kaspersky Administration Kit, см. п. 21.2 на стр. 332.

A.6. Параметры карантина

Карантин имеет следующие параметры:

- папка карантина (см. п. A.6.1 на стр. 438);
- максимальный размер карантина (см. п. A.6.2 на стр. 439);
- порог свободного места в карантине (см. п. A.6.3 на стр. 440);
- папка для восстановления (см. п. A.6.4 на стр. 441).

A.6.1. Папка карантина

Параметр	Папка карантина.
Описание	Вы можете указать папку-местоположение карантина, отличную от папки карантина, установленной по умолчанию.
Возможные значения	Укажите папку на локальном диске защищаемого сервера (имя папки и полный путь к ней). Антивирус начнет помещать объекты в указанную параметром папку, как только вы сохраните новое значение параметра. Если указанная папка карантина не существует или недоступна, Антивирус перейдет к использованию папки карантина, установленной по умолчанию. Указывая путь к папке карантина, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. В кластерном окружении не указывайте в качестве папки карантина папку на кворумном диске или кластерных дисках.
Значение по умолчанию	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ Quarantine\ Вы можете использовать переменную окружения Антивируса %KAVWSEEAPPDATA%, чтобы указать папку Антивируса %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 11.8 на стр. 185;
- в приложении Kaspersky Administration Kit, см. п. 20.4.2 на стр. 315.

A.6.2. Максимальный размер карантина

Параметр	Максимальный размер карантина.
Описание	Значение этого параметра задает максимальный размер карантина – общий объем данных в папке карантина. Параметр **Максимальный размер карантина** носит информационный характер. Он не ограничивает размер папки карантина, а только является критерием регистрации события и позволяет администратору следить за состоянием карантина. После того как максимальный размер карантина достигнут, Антивирус продолжает помещать подозрительные объекты на карантин. Вы можете настроить уведомление о том, что максимальный размер карантина превышен. Антивирус отправляет уведомление, как только общий объем данных в папке карантина достигнет указанного значения (информацию о настройке уведомлений содержит Глава 15 на стр. 234). Рекомендуемое значение: 200 МБ.
Возможные значения	1– 999 МБ.
Значение по умолчанию	Не установлен.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 11.8 на стр. 185;
- в приложении Kaspersky Administration Kit, см. п. 20.4.2 на стр. 315.

A.6.3. Порог свободного места в карантине

Параметр	Порог свободного места в карантине.
Описание	Этот параметр используется вместе с параметром **Максимальный размер карантина**. Параметр **Порог свободного места в карантине** носит информационный характер. Он не ограничивает размер папки карантина, но позволяет получать информацию о скором заполнении карантина. Если объем свободного места в папке карантина становится меньше заданного порога, Антивирус регистрирует событие **Превышен порог свободного места в карантине** и продолжает изолировать подозрительные объекты. Вы можете настроить уведомления о событии **Превышен порог свободного места в карантине** (информацию о настройке уведомлений содержит Глава 15 на стр. 234).
Возможные значения	Укажите объем в МБ; он должен быть меньше значения, установленного параметром **Максимальный размер карантина**. Рекомендуемое значение: 50 МБ.
Значение по умолчанию	Не установлен.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 11.8 на стр. 185;
- в приложении Kaspersky Administration Kit, см. п. 20.4.2 на стр. 315.

A.6.4. Папка для восстановления

Параметр	Папка для восстановления.
Описание	Значение этого параметра задает специальную папку для восстановленных объектов на защищаемом сервере. При восстановлении объекта вы сможете выбрать, куда сохранить восстановленный объект: в исходное местоположение, в специальную папку для восстановленных объектов на защищаемом сервере или в указанную другую папку (на компьютере, на котором установлена консоль Антивируса, или сетевую).
Возможные значения	Укажите папку на локальном диске защищаемого сервера (имя папки и полный путь к ней). Указывая путь к папке для восстановления, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. Если вы управляете Антивирусом на защищаемом сервере через консоль MMC, установленную на удаленном рабочем месте администратора, то вы должны входить в группу локальных администраторов на защищаемом сервере, чтобы просматривать папки на нем.
Значение по умолчанию	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Restored\ Вы можете использовать переменную окружения Антивируса %KAVWSEEAPPDATA%, чтобы указать папку Антивируса %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 11.8 на стр. 185;
- в приложении Kaspersky Administration Kit, см. п. 20.4.2 на стр. 315.

A.7. Параметры резервного хранилища

Резервное хранилище имеет следующие параметры:

- папка резервного хранилища (см. п. A.7.1 на стр. 442);
- максимальный размер резервного хранилища (см. п. A.7.2 на стр. 444);
- порог свободного места в резервном хранилище (см. п. A.7.3 на стр. 445);
- папка для восстановления (см. п. A.7.4 на стр. 446).

A.7.1. Папка резервного хранилища

Параметр	Папка резервного хранилища.
Описание	Вы можете задать папку-местоположение резервного хранилища, отличную от папки, установленной по умолчанию.
Возможные значения	Укажите папку на локальном диске защищаемого сервера (имя папки и полный путь к ней). Антивирус перейдет к использованию указанной параметром папки, как только вы сохраните новое значение параметра. Если указанная папка резервного хранилища не существует или недоступна, Антивирус перейдет к использованию папки резервного хранилища, установленной по умолчанию. Указывая путь к папке резервного хранилища, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. В кластерном окружении не указывайте в качестве папки резервного хранилища папку на кворумном диске кластера или кластерных дисках. Если вы управляете Антивирусом на защищаемом сервере через консоль MMC, установленную на удаленном рабочем месте администратора, то вы должны входить в группу локальных администраторов на защищаемом сервере, чтобы просматривать папки на нем.

Значение по умолчанию	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Backup\ Вы можете использовать переменную окружения Антивируса %KAVWSEEAPPDATA%, чтобы указать папку Антивируса %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 12.5 на стр. 199;
- в приложении Kaspersky Administration Kit, см. п. 20.5.2 на стр. 318.

A.7.2. Максимальный размер резервного хранилища

Параметр	Максимальный размер резервного хранилища.
Описание	Значение этого параметра задает максимальный размер резервного хранилища карантина – общий объем данных в папке резервного хранилища. Параметр **Максимальный размер резервного хранилища** носит информационный характер. Он не ограничивает размер папки резервного хранилища, а только является критерием события и позволяет администратору следить за состоянием хранилища. После того как максимальный размер резервного хранилища достигнут, Антивирус продолжает сохранять копии зараженных файлов в резервном хранилище. Вы можете настроить уведомление администратора о том, что максимальный размер резервного хранилища превышен. Антивирус отправляет уведомление, как только общий объем данных в резервном хранилище достигнет указанного значения (информацию о настройке уведомлений содержит Глава 15 на стр. 234). Рекомендуемое значение: 200 МБ.
Возможные значения	1– 999 МБ.
Значение по умолчанию	Не установлен.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 12.5 на стр. 199;
- в приложении Kaspersky Administration Kit, см. п. 20.5.2 на стр. 318.

A.7.3. Порог свободного места в резервном хранилище

Параметр	Порог свободного места в резервном хранилище.
Описание	Этот параметр используется вместе с параметром **Максимальный размер резервного хранилища**. Этот параметр носит только информационный характер. Он не ограничивает размер папки резервного хранилища, но позволяет получать информацию о его скором заполнении. Если объем свободного места в резервном хранилище становится меньше заданного порога, Антивирус регистрирует событие **Превышен порог свободного места в резервном хранилище** и продолжает резервировать зараженные файлы. Вы можете настроить уведомления о событиях этого типа (информацию о настройке уведомлений содержит Глава 15 на стр. 234).
Возможные значения	Укажите объем в МБ; он должен быть меньше значения, установленного параметром **Максимальный размер резервного хранилища**. Рекомендуемое значение: 50 МБ.
Значение по умолчанию	Не установлен.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 12.5 на стр. 199;
- в приложении Kaspersky Administration Kit, см. п. 20.5.2 на стр. 318.

A.7.4. Папка для восстановления

Параметр	Папка для восстановления.
Описание	Значение этого параметра задает специальную папку для восстановленных объектов на локальном диске защищаемого сервера. При восстановлении файла вы сможете выбрать, куда сохранить восстановленный файл: в исходную папку, в специальную папку для восстановленных объектов на защищаемом сервере или в другую указанную папку (на компьютере, на котором установлена консоль Антивируса, или сетевую). Если вы управляете Антивирусом на защищаемом сервере через консоль MMC, установленную на удаленном рабочем месте администратора, то вы должны входить в группу локальных администраторов на защищаемом сервере, чтобы просматривать папки на нем.
Возможные значения	Укажите папку на локальном диске защищаемого сервера (имя папки и полный путь к ней). Указывая путь к папке для восстановления, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
Значение по умолчанию	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Restored\ Вы можете использовать переменную окружения Антивируса %KAVWSEEAPPDATA%, чтобы указать папку Антивируса %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\.

О том, как настроить параметр:

- в консоли Антивируса в MMC, см. п. 12.5 на стр. 199;
- в приложении Kaspersky Administration Kit, см. п. 20.5.2 на стр. 318.

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 комплексов, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну.

ПБЗИ «Крипто-Си» предназначена для использования в системах комплексной защиты конфиденциальной информации по типу КС1 и имеет сертификат соответствия ФСБ № СФ/114-0960 от 1 января 2007 г.

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 98/NT/XP/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: mailto:info@cryptoex.ru

ПРИЛОЖЕНИЕ C. 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.

C.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 области уведомлений панели задач 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 облас-

тей 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 оперативной 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 Work Space 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.

C.2. Наши координаты

Если у вас возникнут вопросы, вы можете обратиться к нашим дистрибьюторам или в ЗАО «Лаборатория Касперского». Вам будут предоставлены подробные консультации по телефону или электронной почте.

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 бизнес-продуктов:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 в рабочие дни с 10 до 18:30 часов по московскому времени (GMT +3)
Электронная система Help-Desk:	http://support.kaspersky.ru/helpdesk.html
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

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ