Лабораторные 7-8: Обеспечение антивирусной защиты сетевой инфраструктуры на основе продуктов компании «Лаборатория Касперского»

СОДЕРЖАНИЕ

5. Обеспечение антивирусной защиты сетевой инфраструктуры на основе продуктов компании «Лаборатория Касперского»

В этом занятии будет кратко рассмотрена классификация вредоносных программ и приведены основы практического применения следующих продуктов компании «Лаборатория Касперского»:

- Антивирус Касперского® для WindowsWorkstations.
- Антивирус Касперского® для WindowsFileServers.
- Kaspersky® Administration Kit.

Прежде всего

Для изучения материалов этого занятия необходимо:

•Два компьютера объединенных в один домен test.local. Один под управлением операционной системы WindowsXPProfessional. Второй под управлением операционной системы Windows Server 2003.

•CD-ROMдиск с дистрибутивами продуктов из состава Kaspersky® CorporateSuite: Антивирус Касперского® для WindowsWorkstations, Антивирус Касперского® для WindowsFileServers, Kaspersky® AdministrationKit.

5.1. Угрозы компьютерной безопасности

Ни для кого не секрет, что вредоносные программы являются одной из самых серьезных проблем мирового IT-сообщества. Мировой ущерб от вирусов постоянно растет (см. табл. 5.1). На пресс-конференции «Вирусные итоги 2005 года», проведенной 24.01.2006 «Лабораторией Касперского», Евгений Касперский так охарактеризовал текущую ситуацию с распространением вредоносных программ: «Раньше было плохо, сейчас стало совсем плохо. Десять лет назад вирусы писали для удовольствия, а сегодня этим занимаются, чтобы заработать деньги»[1].

Таблица 5.1

Мировой ущерб от вирусов [1]

Год	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
Мировой ущерб, млрд. долл.	0,5	1,8	3,3	6,1	12,1	17,1	13,2	11,1	13,0	16,7

Чтобы эффективно организовать защиту информации в организации, необходимо знать все угрозы компьютерной безопасности и пути их распространения. «Лаборатория Касперского» выделяет следующие источники угроз информационной безопасности [2]:

1. Человеческий фактор. Это угрозы связанные с действиями человека, имеющего санкционированный или несанкционированный доступ к информации. Выделяют:

1.а. Внешние угрозы. Это действия кибер-преступников, хакеров, интернет-мошенников, недобросовестных партнеров, криминальных структур.

1.б. Внутренние угрозы. Это умышленные или случайные действия персонала компании или домашних пользователей.

2. Технический фактор. Это угрозы связанные с техническими проблема ми - физическое и моральное устаревание использующегося оборудования, некачественные программные и аппаратные средства обработки информации.
3. Стихийный фактор. Это природные катаклизмы, стихийные бедствия и прочие форс-мажорные обстоятельства, независящие от людей.

Антивирусные продукты «Лаборатории Касперского» предназначены для борьбы с внешними угрозами, связанными с деятельностью человека.

«Лаборатория Касперского» выделяет следующие источники распространения угроз информационной безопасности [2]:

- Интернет.
- Интранет.
- Электронная почта.
- Съемные носители информации.

«Лаборатория Касперского» выделяет следующие категории вредоносного программного обеспечения[2,3]:

- Сетевые черви.
- Классические компьютерные вирусы.
- Троянские программы.
- Хакерские утилиты и прочие вредоносные программы.

Чтобы не нарушать чужие авторские права и не злоупотреблять цитированием источников, подробнее об этих категориях, а также о признаках заражения компьютера, действиях при их обнаружении и профилактике заражения компьютера Вы можете прочитать на сайте www.viruslist.ruили в документации к антивирусным продуктам «Лаборатории Касперского» (например, [2]).

5.2. Kaspersky® Corporate Suite

Программный продукт Kaspersky® CorporateSuite - интегрированная система, предназначенная для обеспечения безопасности всех составляющих корпоративной сети вне зависимости от ее масштаба и сложности [4]. В его состав входят следующие приложения [4]:

- для защиты рабочих станций: Антивирус Касперского® для Windows 98/Me, Windows 2000/NT/XPWorkstationи Linux;
- длязащитыфайловыхсерверов: АнтивирусКасперского® дляWindows NT 4.0 Server, Windows 2000 Server/Advanced Server, Windows 2003 Server; Novell Netware, FreeBSD, OpenBSD, Linux, Samba Server;

• для защиты почтовых систем: Антивирус Касперского® для MicrosoftExchangeServer5.5/2000/2003, LotusNotes/Domino, Sendmail, Postfix, Eximи Qmail;

• для защиты каналов выхода в Интернет: Антивирус Касперского® для MSISA-серверов, Антивирус Касперского® для CheckPointFirewall;

• для защиты карманных компьютеров: Антивирус Касперского® для PalmOSи WindowsCE;

• для централизованной установки и управления: Kaspersky® AdministrationKit.

В этом занятии мы рассмотрим возможности и примеры практического использования следующих приложений из состава Kaspersky® CorporateSuite:

- Антивирус Касперского® для WindowsWorkstations.
- Антивирус Касперского® для WindowsFileServers.
- Kaspersky® Administration Kit.

Рассмотрим возможности и системные требования этих продуктов.

5.2.1. Антивирус Касперского® для Windows Workstations

Всё дальнейшее описание базируется на версии 5.0.712. С полным описанием возможностей этого продукта Вы можете ознакомиться в [5]. Перечислим наиболее важные из них [5]:

• Постоянная защита файловой системы от вредоносного кода в режиме мониторинга.

• Поиск и обезвреживание вредоносного кода по требованию пользователя или администратора.

- Проверка электронной почты в режиме мониторинга.
- Проверка потенциально опасного программного обеспечения.

• Постоянная защита офисных приложений, использующих VBA-макросы.

- Постоянная проверка опасных скриптов VBScriptи JavaScript.
- Помещение подозрительных объектов на карантин.

• Создание копии зараженного объекта в резервном хранилище перед лечением и удалением.

• Обновление антивирусных баз и программных модулей, входящих в состав Антивируса, с серверов обновлений Лаборатории Касперского; создание резервной копии всех обновляемых файлов на случай необходимости отката последнего произведенного обновления.

• Разделение прав администратора безопасности и пользователя рабочей станции, реализованное в двух интерфейсах.

• Централизованное удаленное управление системой антивирусной защиты с помощью дополнительного административного интерфейса под управлением KasperskyAdministrationKit.

В версии Антивируса Касперского 5.0 для WindowsWorkstationsпо сравнению с версиями 4.x произведены следующие изменения[5]:

• Использование нового антивирусного ядра и новых технологий iChecker™ и iStreams™ позволяет значительно сократить объем занимаемой оперативной памяти и увеличить производительность антивирусной защиты по сравнению с версией 4.0.

• Увеличена скорость обновления антивирусных баз за счет автоматического определения наименее загруженного сервера обновлений Лаборатории Касперского; добавлен алгоритм получения оставшейся части обновления в случае обрыва соединения; появилась возможность помещения полученных обновлений в локальный источник для предоставления доступа к ним другим компьютерам сети в целях экономии интернет-трафика.

• Появилась возможность настройки антивирусной защиты с помощью выбора одного из трех предопределенных уровней защиты с настройками, определенными экспертами Лаборатории Касперского: "максимальная защита", "рекомендуемый" и "максимальная скорость".

• Добавлена возможность проверки и обработки потенциально опасного программного обеспечения в режимах постоянной защиты и проверки по требованию.

• Добавлена возможность лечения файлов в архивах ZIP, ARJ, CAB, RAR.

• Появилась возможность проверки почтового трафика по протоколам SMTP/POP3 вне зависимости от используемого почтового клиента, а также возможность лечения почтовых баз MicrosoftOutlooki MicrosoftOutlookExpress.

• Создано резервное хранилище для сохранения копий подозрительных или зараженных объектов, созданных перед их лечением и удалением.

• Усовершенствована работа карантина: появилась возможность ограничения времени хранения подозрительных объектов на карантине. Добавлена возможность отправки данных объектов на исследование в Лабораторию Касперского из интерфейса карантинного хранилища.

Если на Вашем компьютере установлена операционная система WindowsXP, то для оптимальной работы приложения рабочая станция должна соответствовать следующим требованиям [5]:

- Intel Pentium® 300 ЖГц или выше;
- 128 Мб свободной оперативной памяти;
- 50 Мб свободного дискового пространства;
- CD-ROM-устройство;
- Microsoft Internet Explorer версиинениже 5.0.

Требования для компьютеров с другими операционными системами (MSWindows® 98/Me/NTWorkstations4.0/ 2000 Professional) см. в [5].

5.2.2. Антивирус Касперского® для WindowsFileServers

Всё дальнейшее описание базируется на версии 5.0.77. С полным описанием возможностей этого продукта Вы можете ознакомиться в [6]. Возможности Антивируса Касперского® для WindowsFileServersв целом аналогичны возможностям Антивируса Касперского® для WindowsWorkstation. Но существует несколько отличительных особенностей [6]:

• Управление приложением может осуществляться локально из командной строки или с помощью Консоли администрирования, а также удаленно через систему централизованного управления KasperskyAdministrationKit5.0.

• В журнале событий появилась функция установки фильтров регистрируемых событий, по наступлению которых выполняется соответствующее действие: сохранение в WindowsEventLog, уведомление по E-mail, уведомление с помощью NET SEND, выполнение команды операционной системы.

• Не контролируется почтовый трафик по протоколам SMTP/POP3.

Если на Вашем сервере установлена операционная система Windows 2003 Server, то для оптимальной работы приложения сервер должен соответствовать следующим требованиям [6]:

• Intel Pentium или выше;
• 128 Мб свободной оперативной памяти;
• 30 М6 свободного дискового пространства.

Требования для серверов с другими операционными системами (MSWindows® NT4.0 Server, Windows® 2000 Server/AdvancedServer) см. в [6].

5.2.3. Kaspersky® Administration Kit

Приложение Kaspersky® AdministrationKitпредназначено для централизованного решения основных административных задач по управлению системой антивирусной безопасности компьютерной сети предприятия, построенной на основе приложений, входящих в состав продуктов компании Антивирус Касперского BusinessOptimaли KasperskyCorporateSuite. Kaspersky® AdministrationKitподдерживает работу во всех сетевых конфигурациях, использующих протокол TCP/IP [7].

Всё дальнейшее описание базируется на версии 5.0.1152. С полным описанием возможностей этого продукта Вы можете ознакомиться в [7]. Перечислим наиболее важные из них [7]:

• Удаленная централизованная установка приложений, входящих в состав продуктов Лаборатории Касперского, на компьютеры, работающие под управлением операционных систем семейства Windows.
• Управление лицензиями.
• Удаленное централизованное управление всеми приложениями, входя-

компьютерах под управлением операционной системы Windows. В том числе:

- объединение компьютеров в группы администрирования в соответствии с выполняемыми функциями и набором установленных на них приложений;
- централизованную настройку параметров работы приложения путем создания и применения групповых политик;
- индивидуальную настройку параметров работы приложения для отдельных компьютеров при помощи настроек приложения;
- централизованное управление работой приложений путем создания и запуска групповых и глобальных задач;
- построение индивидуальных схем работы приложений путем создания и запуска задач для набора компьютеров из различных групп администрирования.

- Централизованное автоматическое обновление антивирусных баз и модулей приложения на компьютерах без непосредственного обращения каждого компьютера к интернет-серверу Лаборатории Касперского.
- Система получения отчетности.
- Механизм оповещения о событиях в работе приложений. Механизм рассылки почтовых уведомлений.

Приложение KasperskyAdministrationKitсостоит из трех основных компонентов [7]:

• Сервер администрирования (выполняет функции централизованного хранения информации об установленных в сети предприятия приложениях Лаборатории Касперского и управления ими).

• Консоль администрирования (предоставляет пользовательский интерфейс к административным сервисам Сервера и Агента; выполнена в виде компонента расширения к MicrosoftManagementConsole (MMC)).

• Агент администрирования (осуществляет взаимодействие между Сервером администрирования и приложениями Лаборатории Касперского, установленными на конкретном сетевом узле (рабочей станции или сервере)).

В табл. 5.2 представлены требования к аппаратному и программному обеспечению для перечисленных выше компонентов.

Таблица 5.2

Аппаратные и программные требования [7]

'компонент'	**Программные требования**	**Аппаратные требования**
Сервер администрирования	• MSDE2000 с установленным ServicePack3 или MSSQLServer 2000 с установленным ServicePack 3; • Windows 2000 с установленными Service Pack 1, 2, 3, 4; Windows XP с	• процессор IntelPentiumIIIс частотой 800 МГц или выше; • объем оперативной памяти 128 МБ; • объем свободной (доступ-

	установленнымService Pack 1, Windows 2003 Server; Windows NT4 сустановленнымService Pack 6a.	ной) памяти на диске 400 МБ.
Консоль администрирования	Windows 2000 сустановленнымService Pack 1, 2, 3, 4; Windows XP сустановленнымService Pack 1; Windows 2003 Server; Windows NT4 сустановленнымService Pack 6a.	• процессор IntelPentiumII с частотой 400 МГц или выше; • объем оперативной памяти 64 МБ; • объем свободной (доступной) памяти на диске 10 МБ
Агент администрирования	Windows 98; Windows ME; Windows 2000 сустановленнымService Pack 1, 2, 3, 4; Windows NT4 сустановленнымService Pack 6a; Windows XP сустановленнымService Pack 1; Windows 2003 Server	• процессор IntelPentiumc частотой 233 МГц или выше; • объем оперативной памяти 32 МБ; • объем свободной (доступной) памяти на диске 10 МБ.

Таким образом, для использования Kaspersky® AdministrationKitВам необходимо:

1. Установить сервер администрирования на один из серверов в Вашей организации.
2. Установить необходимое количество консолей администрирования на компьютеры, с которых Вы будете управлять сервером администрирования. Это может быть рабочее место администратора и резервная консоль на компьютере где установлен сервер администрирования.
3. На каждый компьютер в Вашей организации, где будут установлены приложения «Лаборатории Касперского», необходимо установить агента администрирования.

5.3. Развертывание антивирусной защиты в сети предприятия

На существующих двух тестовых компьютерах в домене test.localвыполним установку Антивируса Касперского® для WindowsWorkstationsи Антивируса Касперского® для WindowsFileServersпод управлением Kaspersky® AdministrationKit. В качестве основы используем последовательность действий предложенную в [8].

Распределим роли тестовых компьютеров следующим образом:

1. serverOl- контроллер домена, почтовый сервер, рабочее место администратора.
2. clientOl - пользовательская рабочая станция.

Исходя из вышеописанного распределения ролей, на компьютеры будет установлено следующее программное обеспечение.

Сервер serverOl.test.local:

1. Службу почтового сервера.
2. Почтовый клиент.
3. MSDE 2000.
4. Kaspersky® AdministrationKit(сервер и консоль администрирования).

5. Агент администрирования.
6. Антивирус Касперского® для WindowsFileServers.

Рабочая станция clientOl.test.local:

1. Почтовый клиент.
2. Агент администрирования.
3. Антивирус Касперского® для Windows Workstations

Такое распределение ролей призвано минимизировать аппаратные требования при использовании виртуальных машин. В реальной обстановке рабочее место администратора должно быть развернуто на отдельном компьютере. В этом случае почтовый клиент и консоль администрирования будут вынесены с сервера на отдельный компьютер.

5.3.1. Установка службы почтового сервера на компьютер SERVER01

Как указывалось выше, Kaspersky® AdministrationKitимеет возможность отправлять уведомления по электронной почте, поэтому нам нужен почтовый сервер, чтобы использовать эту возможность. Для просмотра возможностей антивирусных решений «Лаборатории Касперского» нам подойдет входящий в комплект WindowsServer2003 простой почтовый сервер. Если в Вашей организации уже существует другой почтовый сервер, рекомендуется использовать его.

Для установки почтового сервера на компьютере `SERVER01` запустите «Мастер настройки сервера». Для этого выполните команду «Пуск | Программы | Администрирование | Управление данным сервером» и в появившемся окне нажмите «Добавить или удалить роль». На странице «Предварительные шаги» нажмите кнопку «Далее». На странице «Роль сервера» выберите роль «Почтовый сервер (POP3, SMTP)» и нажмите кнопку «Далее». На странице «Настройка службы POP3» укажите «Метод проверки подлинности:» - «Интегрированные с ActiveDirectory» и «Имя домена электронной почты:» - «`test.local`» (без кавычек). На странице «Сводка выбранных параметров» нажмите «Далее». После завершения установки, нажмите кнопку «Готово».

Почтовый сервер установлен. Необходимо создать три почтовых ящика: `admin@test.local`, `user01@test.local` и `user02@test.local`. Первый почтовый ящик будет использоваться для получения уведомлений от Сервера администрирования, остальные для демонстрации возможностей Антивируса Касперского.

Откройте окно управления почтовым сервером. Для этого выполните «Пуск | Программы | Администрирование | Служба POP3». В левой части окна разверните пункт SERVER01 и вызовите контекстное меню для почтового сервера `test.local`(рис. 5.1). Выполните команду «Создать | Почтовый ящик...». В окне «Добавление почтового ящик» в поле «Имя почтового ящика:» введите `admin`, а в поля «Пароль» и «Подтверждение пароля» введите «`P@ssw0rd`» (без кавычек). Убедитесь что параметр

«Создать пользователя для этого почтового ящика» включен и нажмите «OK». В появившемся окне будут отображены сведения для настройки почтового клиента на использование созданного ящика (рис. 5.2). Запомните или запишите их.

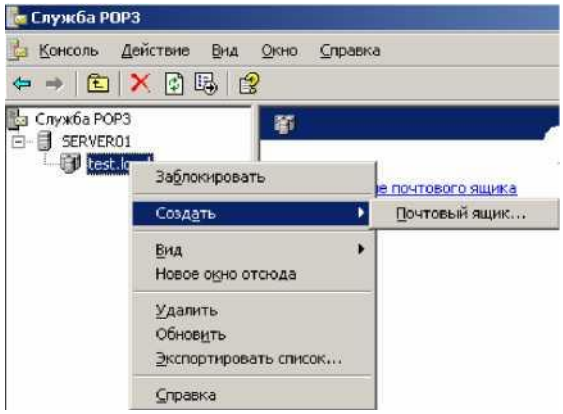

Рис. 5.1. Контекстное меню почтового сервера

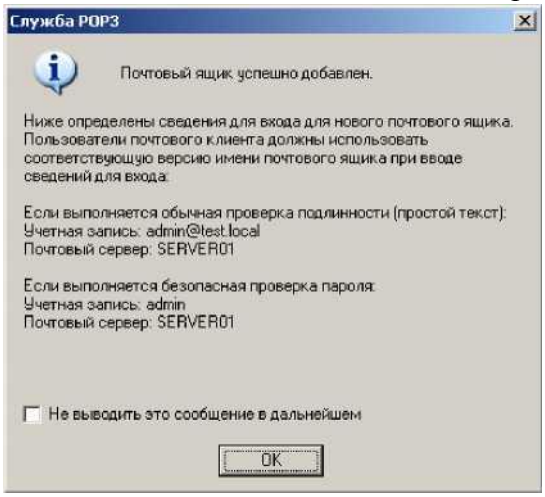

Рис. 5.2. Параметры для настройки почтового клиента Аналогичным образом создайте почтовые ящики `user01` и `user02`.

5.3.2. Настройка почтовых клиентов на компьютерах SERVER01 и CLIENT01

Зарегистрируйтесь на компьютере SERVER01. Запустите программу OutlookExpress. Для этого выполните «Пуск | Программы | OutlookExpress». Выполните команду «Сервис | Учетные записи». Нажмите кнопку «Добавить» и выберите пункт «Почта...». На странице «Введите имя» в поле «Выводимое имя:» введите «Admin» и нажмите «Далее». На странице «Адрес электронной почты Интернета» в поле «Электронная почта:» введите «admin@test.local». На следующей странице в полях «Сервер входящих сообщений» и «Сервер исходящих сообщений» введите «serverOl» и нажмите «Далее». На следующей странице в поле «Учетная запись:» введите «admin@test.local». В поле «Пароль:» введите «P@ssw0rd» и нажмите кнопку «Далее». На последней странице нажмите кнопку «Готово». За©

кройте окно «Учетные записи в Интернете». На панели инструментов нажмите кнопку «Доставить почту». Если сообщений об ошибках не появляется и не запрашивается пароль, то почту Вы настроили верно. Проверьте папку «Входящие». Там не должно быть новых сообщений. Создайте тестовое письмо на адрес user01@test.localи отправьте его.

Аналогичным образом настроим почтовый ящик «user01@test.local» на компьютере clientOl.

Зарегистрируйтесь на компьютере clientOl. Запустите программу OutlookExpress. Для этого выполните «Пуск | Все программы | OutlookExpress». Выполните команду «Сервис | Учетные записи». Нажмите кнопку «Добавить» и выберите пункт «Почта...». На странице «Введите имя» в поле «Выводимое имя:» введите «UserOl» и нажмите «Далее». На странице «Адрес электронной почты Интернета» в поле «Электронная почта:» введите «user01@test.local». На следующей странице в полях «Сервер входящих сообщений» и «Сервер исходящих сообщений» введите «serverOl» и нажмите «Далее». На следующей странице в поле «Учетная запись:» введите «user01@test.local». В поле «Пароль:» введите «P@ssw0rd» и нажмите кнопку «Далее». На последней странице нажмите кнопку «Готово». Закройте окно «Учетные записи в Интернете». На панели инструментов нажмите кнопку «Доставить почту». Если сообщений об ошибках не появляется и не запрашивается пароль, то почту Вы настроили верно. Проверьте папку «Входящие». Там должно быть одно новое тестовое письмо от адресата «Admin».

5.3.3. Установка MSDE 2000 на компьютер SERVER01

Итак, подготовительные действия завершены. Переходим к установке Kaspersky® AdministrationKitна компьютер SERVER01. Как уже было указано ранее, перед его установкой необходимо установить MSDE2000 или SQLServer. ВкомплектесKaspersky® Administration Kit поставляетсяMSDE 2000 cService Pack 3. Выполним его установку.

Примечание: Использование MSDE, поставляемого в комплекте с Kaspersky® AdministrationKit, возможно только для работы Kaspersky® AdministrationKit[7,8].

Зарегистрируйтесь на компьютере SERVER01 с правами администратора. Запустите на выполнение файл msde2ksp3ru.exe. Следуйте указаниям мастера установки. Все предлагаемые параметры можно оставить без изменения.

5.3.4. Установка Сервера администрирования и консоли администрирования на компьютер SERVER01

Зарегистрируйтесь на компьютере SERVER01 с правами администратора домена. Запустите на выполнение файл установки. В нашем случае

это будет kasp5.0.1152_adminkitru.exe. Следуйте указаниям мастера установки (см. рис. 5.3).

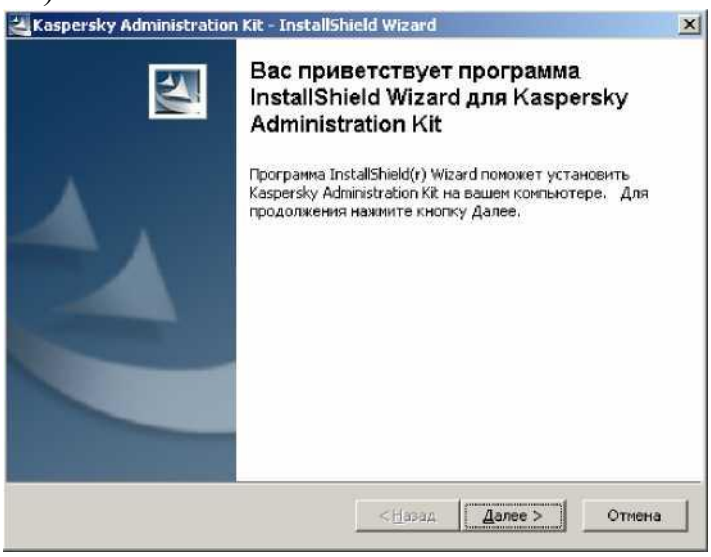

Рис. 5.3. Приветствие программы InstallShieldWizardНажмите кнопку «Далее». В появившемся окне выберите путь для сохранения распакованного дистрибутива (рис. 5.4). Нажмите «Далее».

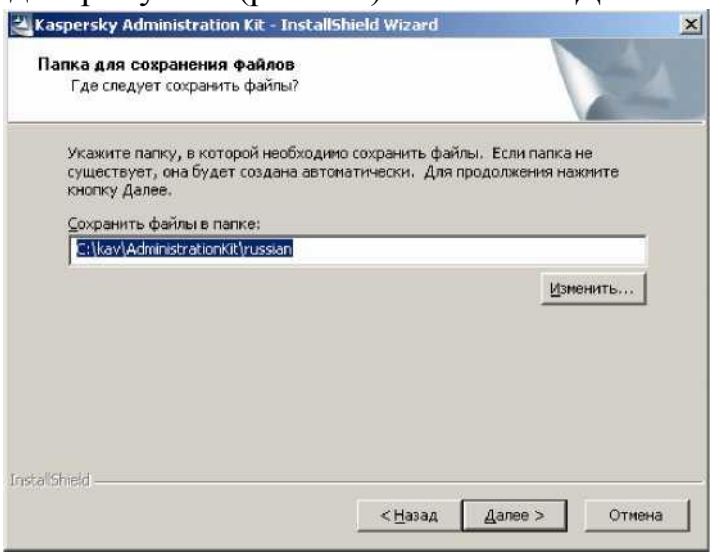

Рис. 5.4. Выбор папки для сохранения файлов После распаковки дистрибутива, на экране появится приветствие Мастера установки (рис. 5.5). Нажмите кнопку «Далее». Ознакомьтесь с лицензионным соглашением и если Вы его принимаете, нажмите кнопку «Да». На следующей странице введите данные о пользователе и организации обладающей лицензией на использование программы. Нажмите кнопку «Далее».

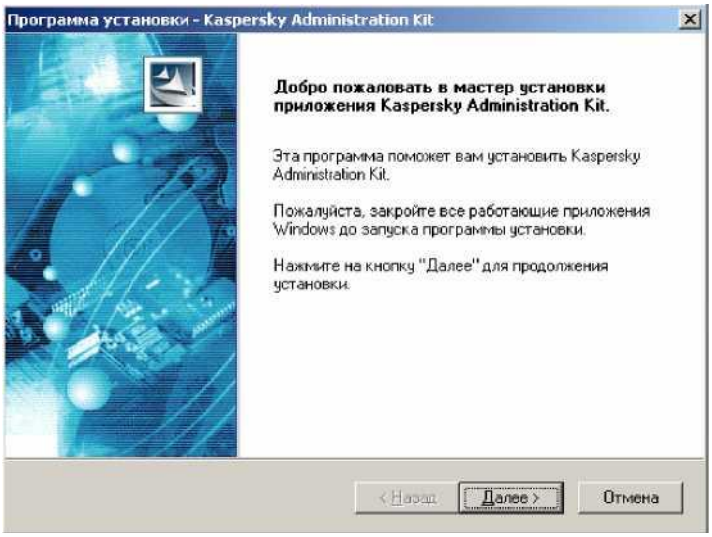

Рис. 5.5. Приветствие мастера установки KasperskyAdministrationKitНа следующей странице укажите каталог для установки программы (рис. 5.6). По умолчанию, программа будет устанавливаться в папку «%ProgramFiles%\KasperskyLab\KasperskyAdministrationKit\». Нажмите кнопку «Далее».

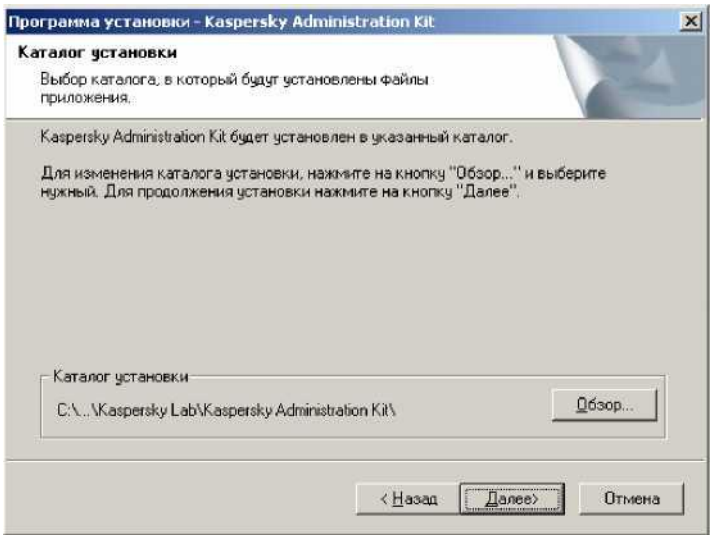

Рис. 5.6. Выбор каталога установки

На странице выбора компонентов приложения для установки выберите те компоненты, которые необходимо установить (рис. 5.7). Если Вы планируете установить только консоль администрирования, то выключите компонент «Сервер администрирования». В нашем случае мы будем устанавливать оба компонента на server01, поэтому нажимаем кнопку «Далее».

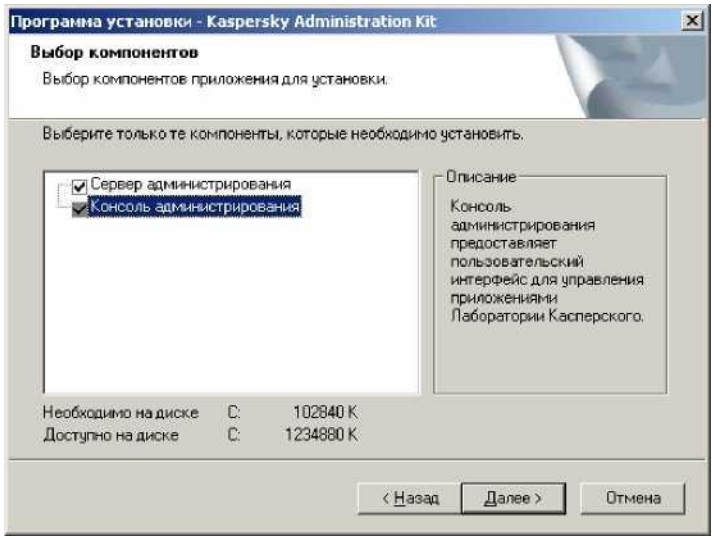

Рис. 5.7. Выбор компонентов для установки Так как мы выбрали установку Сервера администрирования, на следующей странице нам предлагается выбрать учетную запись для запуска службы Сервера администрирования (рис. 5.8). Только при использовании учетной записи пользователя с правами администратора домена можно использовать все возможности Kaspersky® AdministrationKit[7]. Выбираем вариант «Учетная запись пользователя» и нажимаем кнопку «Далее».

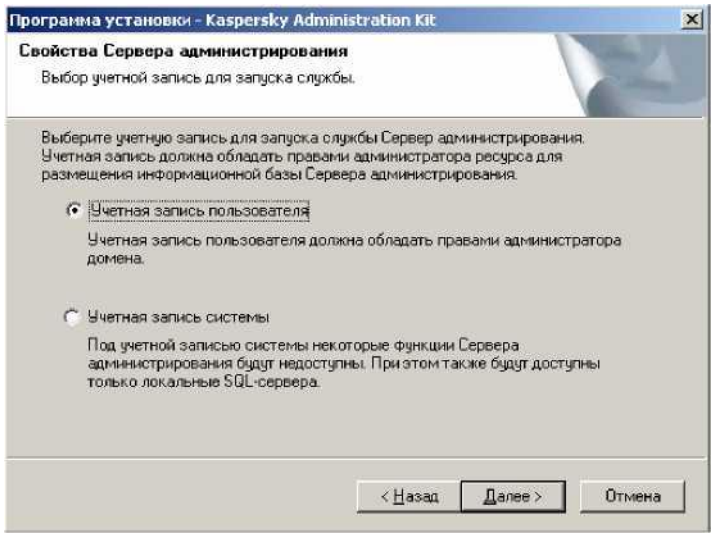

Рис. 5.8. Выбор учетной записи для запуска службы Сервера администрирования

На следующей странице Вам необходимо выбрать уже существующую учетную запись пользователя, которая обладает правами администратора домена и правом «Вход в качестве службы» либо создать новую учетную запись (рис. 5.9).

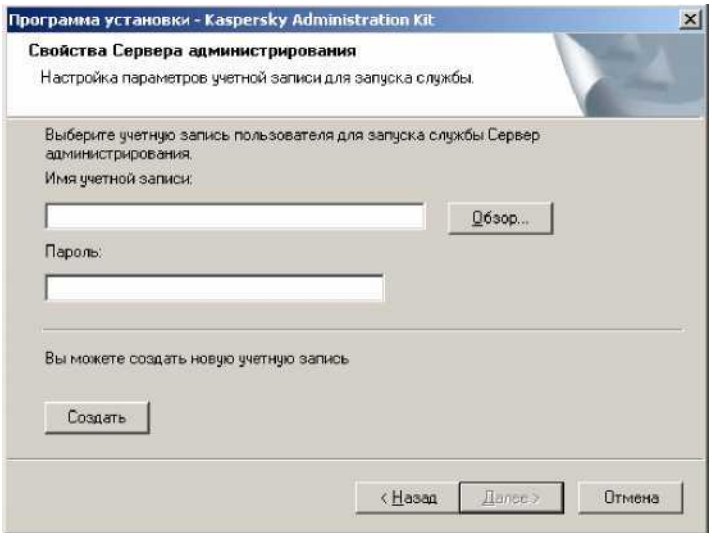

Рис. 5.9. Свойства сервера администрирования Нажмите кнопку «Создать». В появившемся окне укажите имя создаваемой учетной записи и пароль (рис. 5.10). Например, имя - KaspAdminKit, пароль - P@ssw0rd. Нажмите кнопку «Далее».

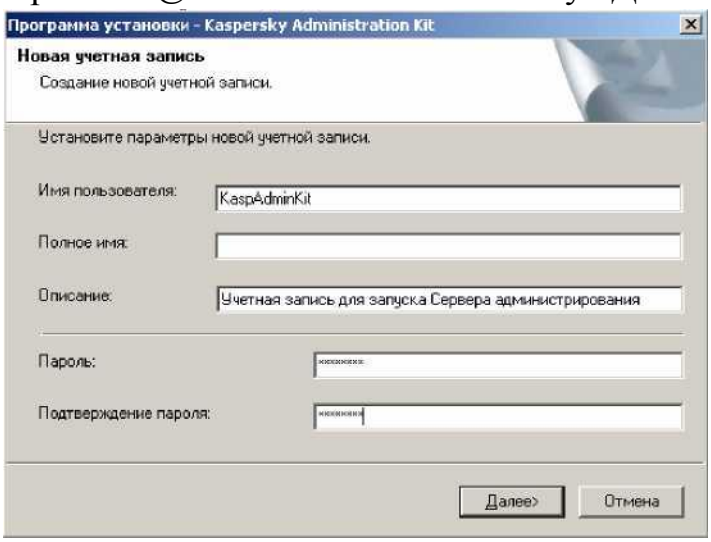

Рис. 5.10. Создание новой учетной записи Вы вернетесь к предыдущему окну, где уже будет указана созданная учетная запись (рис. 5.11). Нажмите кнопку «Далее».

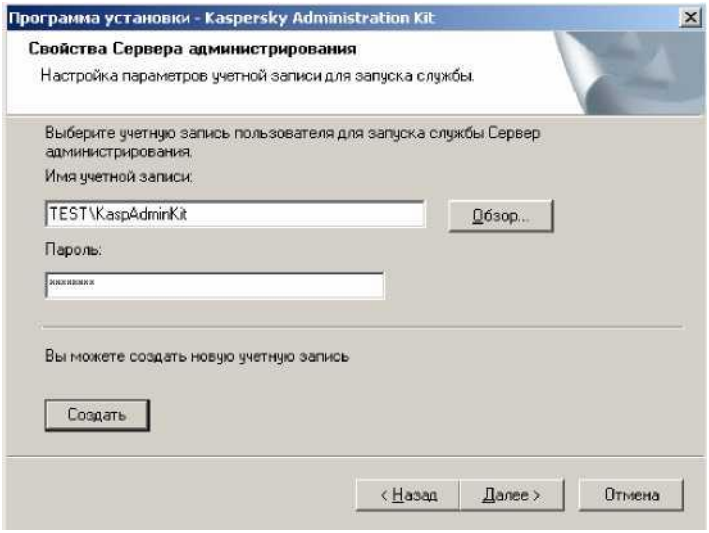

Рис. 5.11. Свойства сервера администрирования На экране появится информационное сообщение о том, какие права будут дополнительно присвоены указанной Вами учетной записи (рис. 5.12). Нажмите кнопку «ОК».

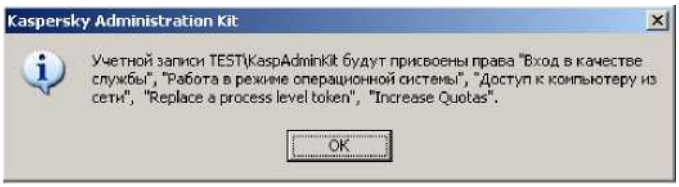

Рис. 5.12. Информационное сообщение

На следующей странице (см. рис. 5.13) Вам будет предложено определить ресурс (MSDEили MicrosoftSQL-сервер), который будет использоваться для размещения информационной базы данных Сервера администрирования и имя базы данных [7]. Так как мы используем MSDE, представленные на экране данные нам подходят. Нажмите кнопку «Далее».

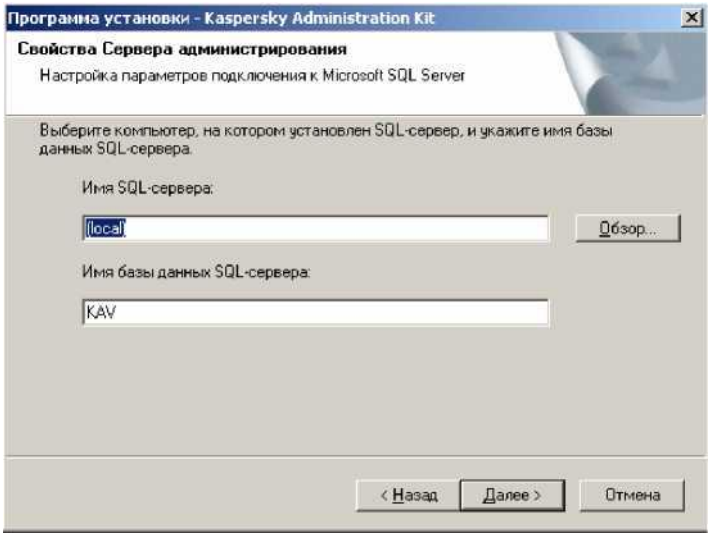

Рис. 5.13. Параметры подключения к MicrosoftSQL-серверу

На следующей странице Вам будет предложено выбрать режим SQL-аутентификации (рис. 5.14). Оставляем вариант по умолчанию и нажимаем кнопку «Далее».

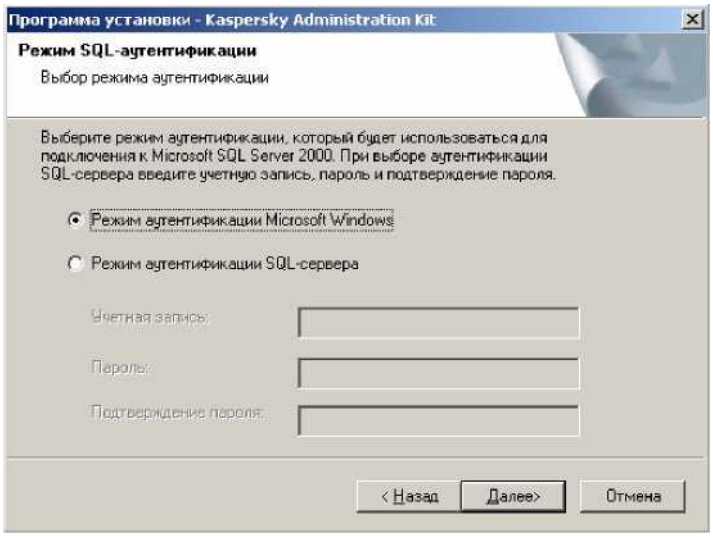

Рис. 5.14. Выбор режима SQL-аутентификации На следующей странице Вам будет предложено указать папку общего доступа для хранения инсталляционных пакетов и обновлений для приложений «Лаборатории Касперского» (рис. 5.15). В этой папке также будет храниться инсталляционный пакет Агента администрирования, который необходим для связи клиентских компьютеров с Сервером администрирования (см. п. 5.2.3). К данному ресурсу будет открыт общий доступ на чтение для всех пользователей. По умолчанию предлагается создать новую общую папку по адресу «%ProgramFiles%\KasperskyLab\KasperskyAdministrationKit\Share» и назначить ей имя SHARE. Изменим имя на «AVP- SHARE» и нажмем кнопку «Далее».

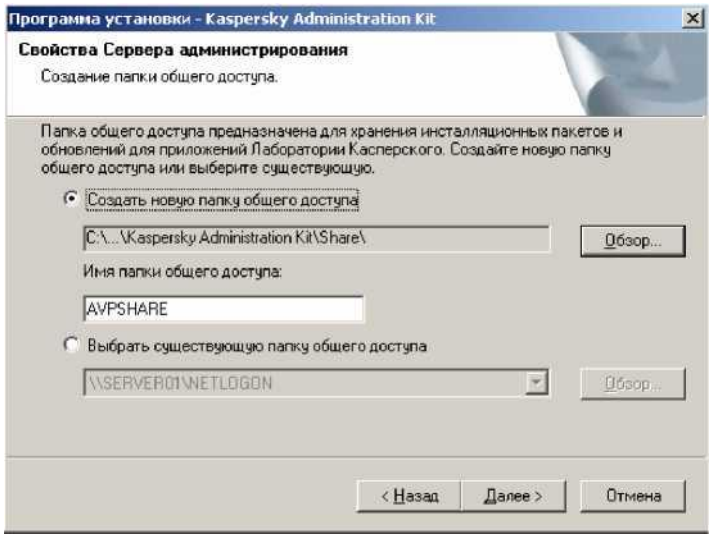

Рис. 5.15. Создание папки общего доступа На следующей странице Вам будет предложено указать номера портов для подключения к Серверу администрирования (рис. 5.16). Если на ком

пьютере, где установлен Сервер администрирования, работает межсетевой экран (например, это компьютер под управлением ОС WindowsXPc ServicePack2 или WindowsServer2003 R2), то необходимо открыть указанные порты вручную для нормального функционирования Сервера администрирования. Нажмите кнопку «Далее».

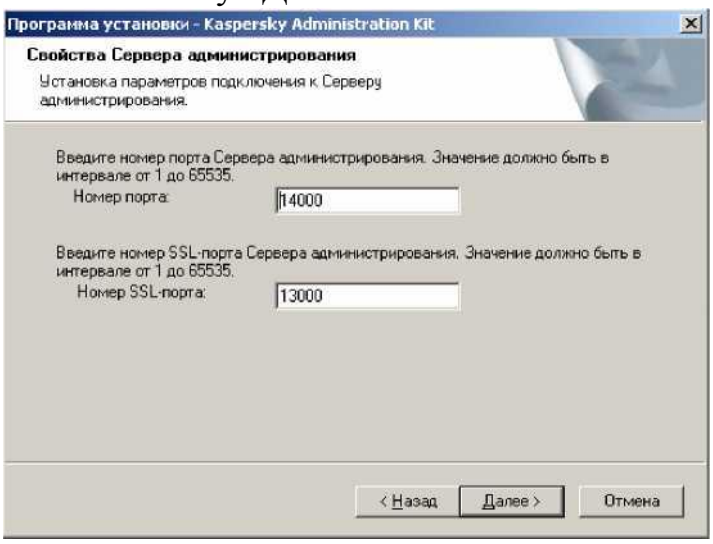

Рис. 5.16. Параметры подключения к Серверу администрирования

На следующей странице (рис. 5.17) Вам будет предложено создать новый сертификат или восстановить его из резервной копии (если Вы переустанавливаете Сервер администрирования). На основании этого сертификата осуществляется аутентификация Сервера администрирования при подключении к нему Консоли администрирования и при обмене информации с клиентскими компьютерами [7]. Если Вы устанавливаете Сервер администрирования в своей организации впервые, то необходимо создать новый сертификат и сохранить резервную копию на случай восстановления Сервера администрирования. Нажмите кнопку «Далее».

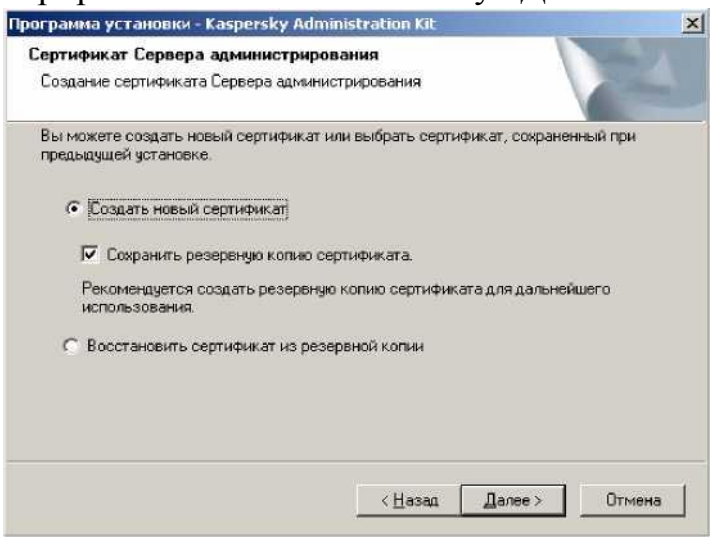

Рис. 5.17. Создание сертификата Сервера администрирования

Если Вы выбрали вариант «Сохранить резервную копию сертификата», то на следующей странице Вам будет предложено указать каталог для создания резервной копии и пароль для его шифрования. Укажите необходимые данные и нажмите кнопку «Далее».

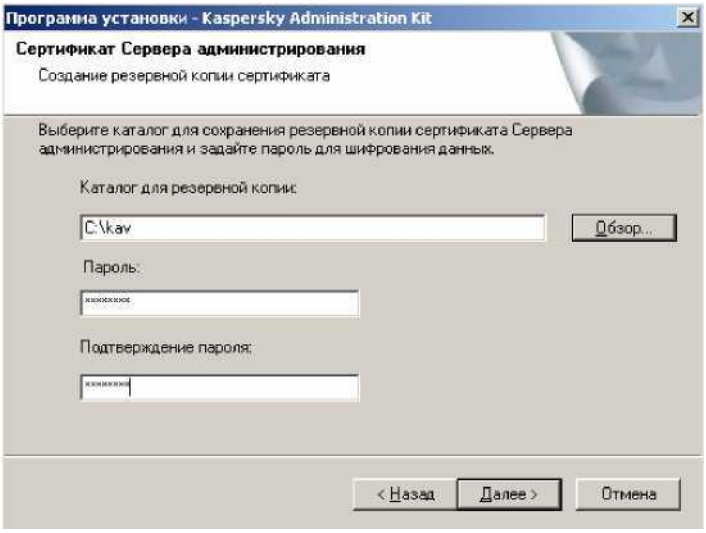

Рис. 5.18. Создание резервной копии сертификата На следующей странице Вам будет предложено ознакомиться с параметрами установки и нажать кнопку «Далее» (рис. 5.19).

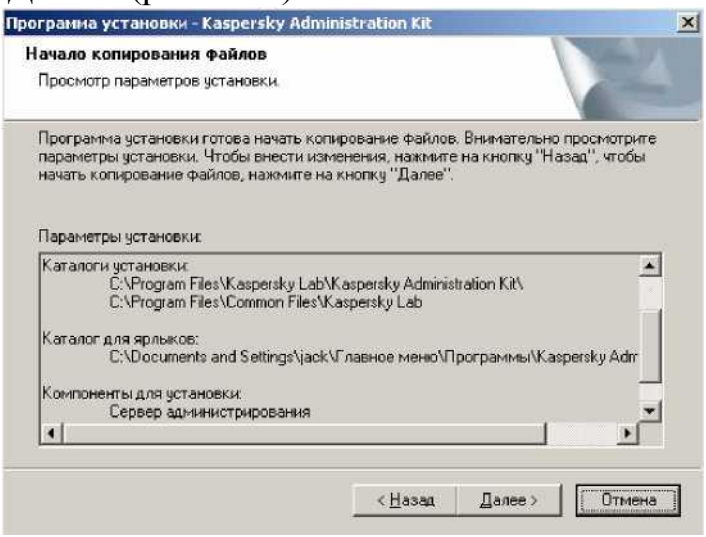

Рис. 5.19. Просмотр параметров установки

После завершения установки (рис. 5.20), нажмите кнопку «Готово».

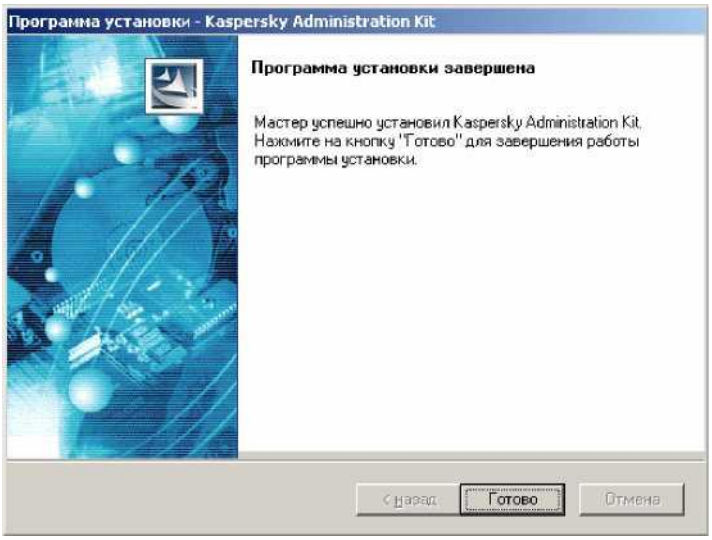

Рис. 5.20. Завершение установки

Сервер администрирования устанавливается на компьютер в качестве службы под именем «KasperskyAdministrationServer».

На компьютере, где установлен Сервер администрирования, также создаются группы локальных пользователей KLAdminsи KLOperators[7]. Так как мы с Вами провели установку Сервера администрирования на контроллер домена, то эти группы были созданы как глобальные группы безопасности в домене. Пользователи, входящие в группу KLAdminsявляются так называемыми **Администраторами логической сети**. Пользователи, входящие в группу KLOperatorsявляются так называемыми **Операторами логической сети**.

Логической сетью называют иерархическую структуру групп администрирования с входящими в их состав клиентскими компьютерами, в которой управление приложениями компании Лаборатория Касперского осуществляется при помощи Kaspersky® AdministrationKit[7].

Администратор логической сети - это пользователь, осуществляющий установку, настройку и обслуживание Kaspersky® AdministrationKit, а также удаленное управление приложениями Лаборатории Касперского на компьютерах логической сети. Он имеет полные права на функциональность, предоставляемую системой администрирования Kaspersky® AdministrationKit[7].

Оператор логической сети - это пользователь, который осуществляет наблюдение за состоянием и работой системы антивирусной защиты, управляемой при помощи Kaspersky® AdministrationKit. Он имеет ограниченный доступ к функциональности системы администрирования Kaspersky® AdministrationKit[7].

С полным перечнем возможностей **Администратора и Оператора логической сети** Вы можете ознакомиться в [7].

Как уже указывалось ранее, Сервер администрирования будет выполняться под указанной при установке учетной записью. В нашем случае это

KaspAdminKit. Соответственно, все операции, которые будут инициировать **Администраторы логической сети**, будут выполняться с правами этой учетной записи (в нашем случае - KaspAdminKit) [7].

5.3.5. Настройка Сервера администрирования

Для того чтобы выполнить первоначальную настройку Сервера администрирования необходимо открыть Консоль администрирования (рис. 5.21). Для этого зарегистрируйтесь на компьютере SERVER01 под учетной записью администратора домена или пользователя входящего в группу KLAdmins. Запустите программу KasperskyAdministrationKit. Для этого выполните «Пуск | Программы | KasperskyAdministrationKit| KasperskyAdministrationKit».

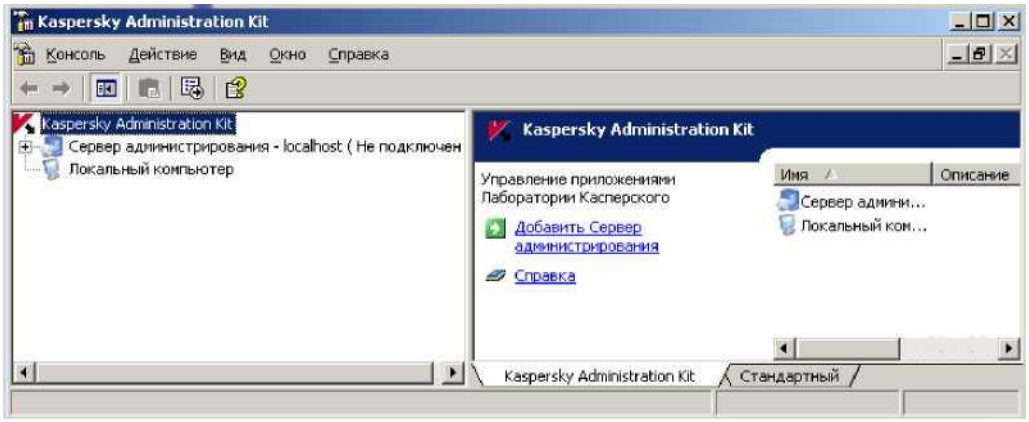

Рис. 5.21. Консоль администрирования

Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования». При первом подключении, Вы увидите предложение запустить Мастер первоначальной настройки (рис. 5.22). Нажмите кнопку «Запустить Мастер первоначальной настройки».

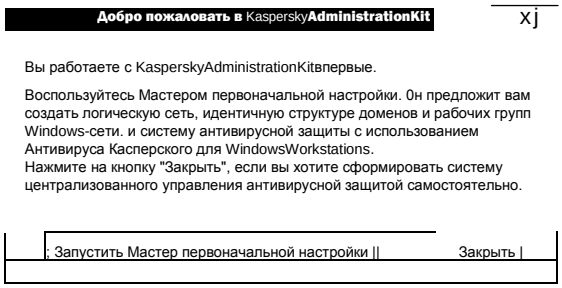

Рис. 5.22. Предложение запустить Мастер первоначальной настройки Мастер первоначальной настройки (рис. 5.23) позволяет сформировать [7]:

• логическую сеть, структура которой будет идентична структуре доменов и рабочих групп Windows-сети;

• параметры рассылки оповещений по электронной почте и средствами NETSENDo событиях, регистрируемых в работе Сервера администрирования, а также всех остальных приложений компании;

• политику и минимальный набор задач самого верхнего уровня иерархии для Антивируса Касперского 5.0 для WindowsWorkstations, а так же глобальную задача получения обновлений Сервером администрирования.

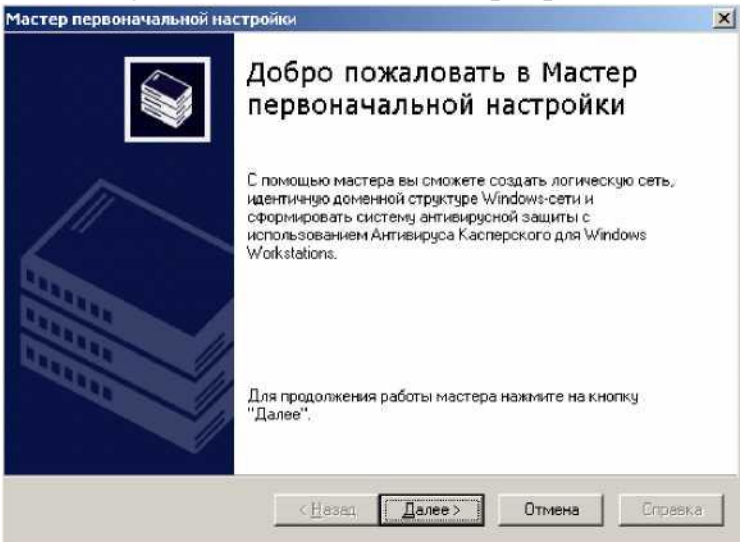

Рис. 5.23. Приветствие Мастера первоначальной настройки Прочитайте приветствие Мастера первоначальной настройки (рис. 5.23) и нажмите кнопку «Далее». Мастер осуществляет опрос сети и на следующей странице отображает сообщение о его завершении (рис. 5.24). Просмотреть результаты опроса сети можно, щелкнув по надписи «Просмотреть результаты опроса сети». Щелкнув по надписи «Просмотреть введение в приложение», Вы получите возможность ознакомиться с «Демонстрацией модели работы приложения KasperskyAdministrationKit».

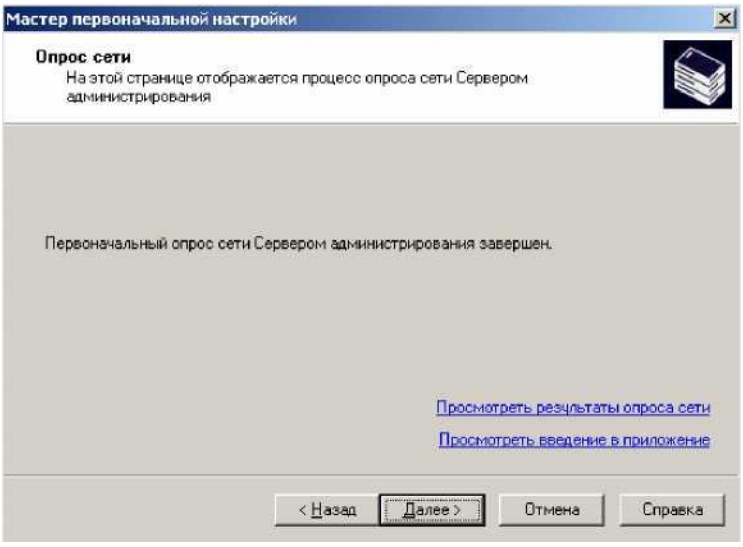

Рис. 5.24. Опрос сети

Нажмите кнопку «Далее». На следующей странице Вам будет предложено выбрать способ создания логической сети (рис. 5.25). Подробнее о предлагаемых способах Вы можете прочитать в документации [7]. Выберите вариант «Сформировать логическую сеть на основе Windows-сети» и нажмите «Далее».

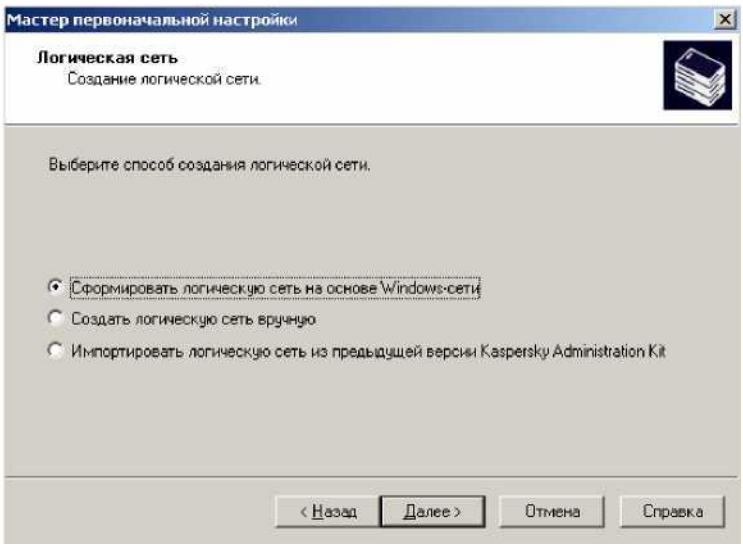

Рис. 5.25. Выбор способа создания логической сетиНа следующей странице Вам будет предложено задать параметры уведомления о событиях, регистрируемых в работе приложений (рис. 5.26). Нажав кнопку «Сообщение» Вы можете отредактировать шаблон отправляемого сообщения. По умолчанию шаблон следующий:
«Событие %EVENT% произошло на компьютере %COMPUTER% в домене %DOMAIN% в %RISE_TIME%
%DESCR%»

Задайте адрес получателя (в нашем примере это admin@test.local), адрес почтового сервера (в нашем примере это server01), номер SMTP-порта (25). Если необходимо, задайте адреса компьютеров-получателей уведомлений средствами NETSENDи нажмите кнопку «Далее».

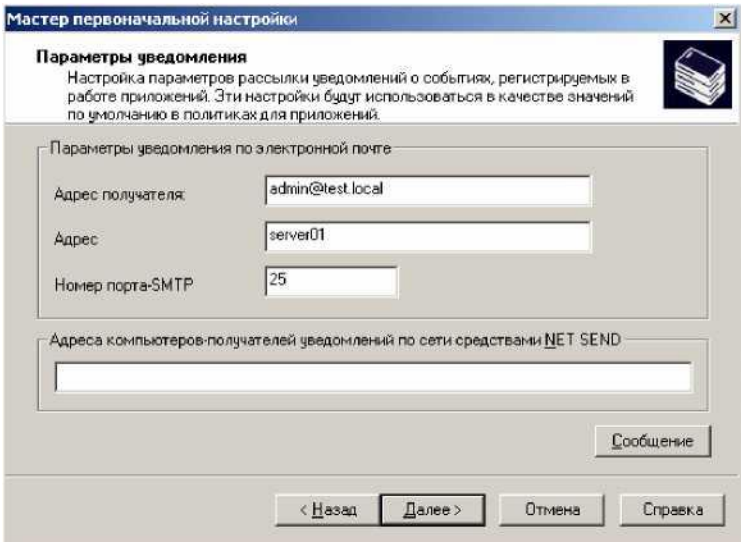

Рис. 5.26. Параметры отправки уведомлений На следующей странице Вам будет сообщено о готовности Мастера к созданию политики и основных групповых задач для Антивируса Касперского для WindowsWorkstationc настройками по умолчанию (рис. 5.27).

Кроме того, будет создана задача получения обновлений Сервером администрирования .

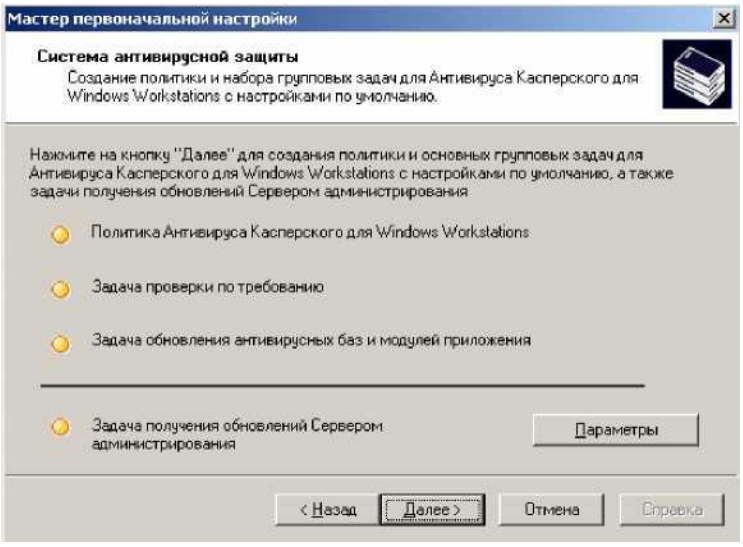

Рис. 5.27. Создание политик и основных групповых задач Нажмите кнопку «Параметры» чтобы задать параметры задачи получения обновлений Сервером администрирования (рис. 5.28). Подробнее о параметрах Вы можете прочитать в документации [7]. Сервер администрирования может получать необходимые Вашей организации обновления для продуктов Лаборатории Касперского из Интернета, а остальные компьютеры в Вашей организации будут получать нужные им обновления не через Интернет, а с Сервера администрирования. Тем самым осуществляется экономия Интернет-трафика. Нажав кнопку «Выбрать», Вы можете задать для каких продуктов серии анти-спам необходимо скачивать обновления (рис. 5.29). Если доступ в Интернет в Вашей организации возможен только через прокси-сервер, то Вам необходимо задать его адрес, нажав кнопку «Параметры LAN...» (рис. 5.30). Нажав кнопку «Добавить...», Вы можете задать дополнительные источники обновления (см. рис. 5.31).

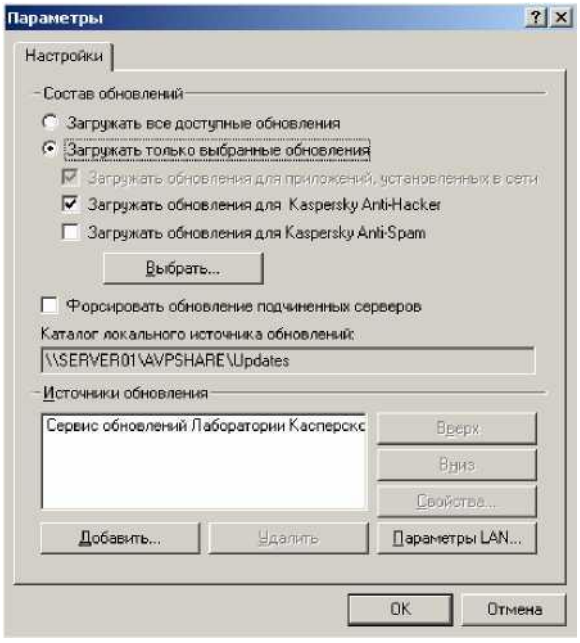

Рис. 5.28. Настройки получения обновлений

Рис. 5.29. Выбор приложений KasperskyAnti-spam

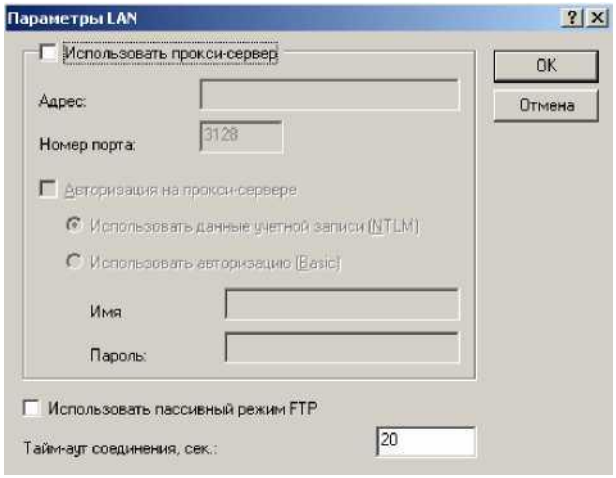

Рис. 5.30. Параметры прокси-сервера

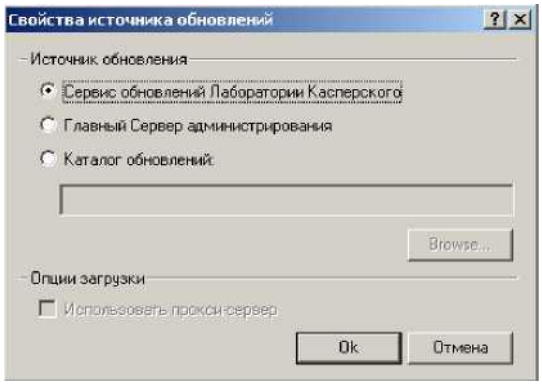

Рис. 5.31. Источники обновления

На странице «Параметры» (см. рис. 5.28) сделаем необходимые изменения и нажмем кнопку «ОК». Вы вернетесь на страницу, представленную на рис. 5.27. Нажмите кнопку «Далее». После завершения работы Мастера, на экране появится соответствующее сообщение (см. рис. 5.32)

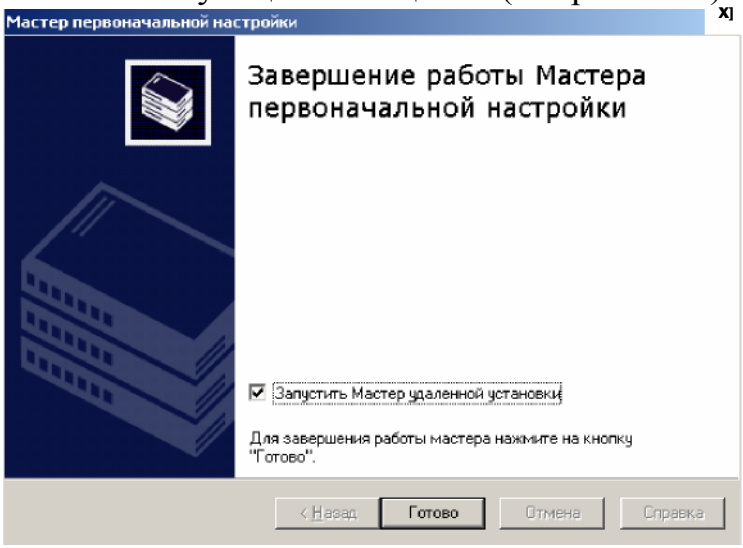

Рис. 5.32. Завершение работы Мастера

Отключите параметр «Запустить Мастер удаленной установки» и нажмите кнопку «Готово».

В результате действий Мастера, окно Консоли администрирования KasperskyAdministrationKitбудет выглядеть следующим образом (см. рис. 5.33).

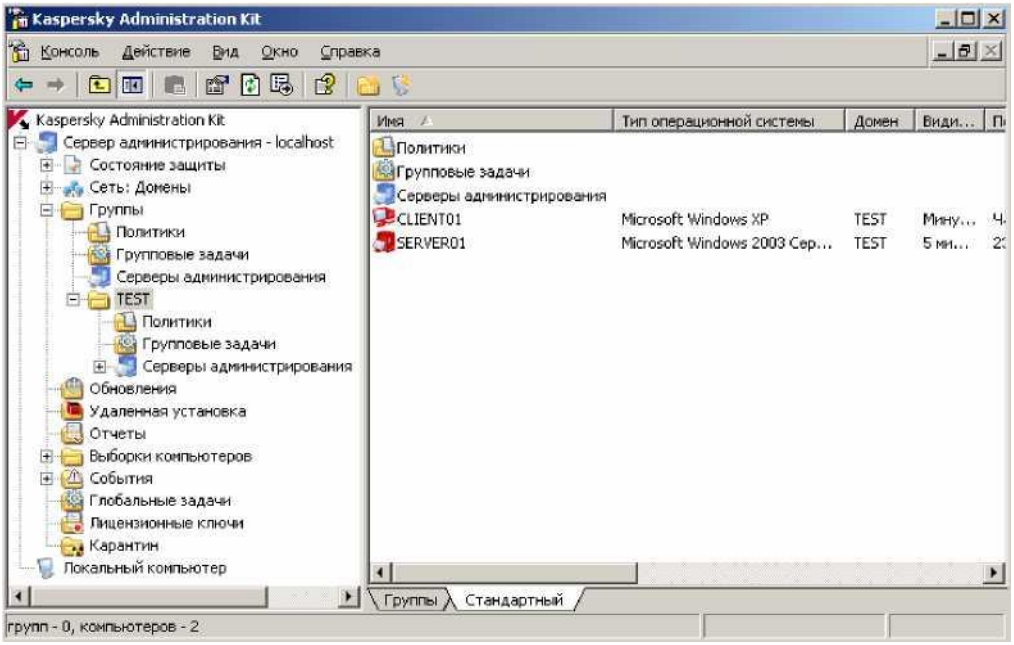

Рис. 5.33. Консоль администрирования

5.3.6. *Удаленная установка приложений с помощью Сервера администрирования*

Кроме локальной установки приложений Лаборатории Касперского на компьютеры существует возможность выполнить удаленную установку приложений с помощью Сервера администрирования. Существует два метода [7]:

1. форсированная установка
2. установка с помощью сценария запуска.

Форсированная установка осуществляется посредством копирования на заданные компьютеры установочных файлов и их последующего удаленного запуска на этих компьютерах. Для успешного выполнения необходимо чтобы Сервер администрирования (точнее учетная запись, под которой он выполняется) обладал правами на удаленный запуск приложений на клиентских компьютерах и возможностью записи на этих компьютерах в административный ресурс admin$. Этот способ используется для компьютеров с установленной ОС MicrosoftWindowsNT/2000/2003/XP. Кроме того, форсированная установка также возможна, если на целевом компьютере уже установлен Агент администрирования. В этом случае, этот метод установки также возможен и на компьютерах с ОС MicrosoftWindows 98/Me. [7]

Если установка производится с помощью административного ресурса admin$, то на клиентском компьютере должны быть открыты соответствующие порты. Для встроенного брандмауэра в WindowsXPSP2 необходимо разрешить исключение «Общий доступ к файлам и принтерам» (порты TCP139, 445 и UDP137, 138) для области соответствующей Серверу администрирования.

Если установка производится с помощью ранее установленного Агента администрирования, то на клиентском компьютере необходимо открыть порт UDP15000.

Если же канал связи между Сервером администрирования и клиентским компьютером перекрыт межсетевым экраном (который в целях безопасности Вы не желаете перенастраивать), то установку на такие компьютеры необходимо производить локально. Либо вначале установить локально Агент администрирования, а после открыть на клиентском компьютере только один порт UDP15000.

Второй метод (**установка с помощью сценария запуска**) позволяет установить для учетных записей конкретных пользователей специальный сценарий входа, который будет запускать программу установки из папки общего доступа на Сервере администрирования при их регистрации в домене. Для успешной работы данного метода необходимо чтобы учетная запись, под которой выполняется Сервер администрирования, обладала правами на изменение сценариев входа в домене. Кроме того, учетная запись пользователя, под которой он регистрируется в домене, должна обладать соответствующими правами для установки приложений на клиентском компьютере. Данный метод Лаборатория Касперского рекомендует для использования на компьютерах с установленной ОС MicrosoftWindows 98/Me[7].

В нашем пособии мы будем использовать только первый метод - **форсированную установку**. Подробнее об описанных вариантах установки, Вы можете прочитать в документации [7].

В реальной обстановке, при небольшом количестве компьютеров в организации, рекомендуем установку Агента администрирования производить локально, а порт UDP15000 открывать с помощью доменной групповой политики. Подробнее об использовании групповой политики для настройки встроенного в WindowsXPSP2 брандмауэра Вы можете прочитать в 6 занятии настоящего пособия.

5.3.7. Удаленная установка Агента администрирования

Выполним форсированную установку Агента администрирования на клиентский компьютер client01. На компьютер server01 устанавливать приложение Агент администрирования нет необходимости, так как там уже установлен Сервер администрирования.

Будем предполагать, что на клиентском компьютере с ОС WindowsXPSP2 уже включено исключение «Общий доступ к файлам и принтерам» и открыт порт UDP15000.

Откройте Консоль администрирования (рис. 5.21). Для этого зарегистрируйтесь на компьютере SERVER01 под учетной записью администратора домена или пользователя входящего в группу KLAdmins. Запустите программу KasperskyAdministrationKit. Для этого выполните «Пуск | Про©

граммы | KasperskyAdministrationKit| KasperskyAdministrationKit». Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования» (рис. 5.33).

В левой части Консоли администрирования выберите узел «Удаленная установка». В правой части окна вызовите контекстное меню элемента «Инсталляционный пакет Агент администрирования» и выполните команду «Установить» (рис. 5.34).

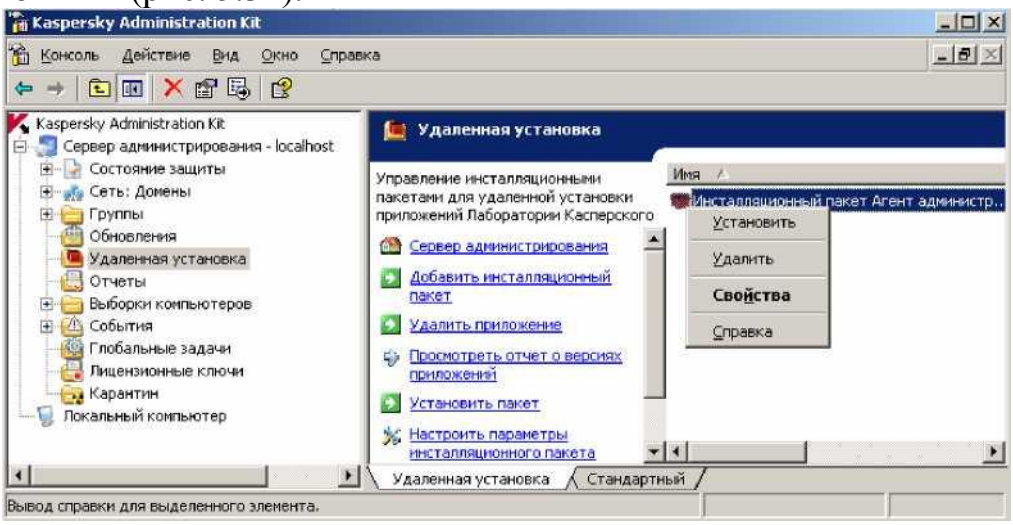

Рис. 5.34. Контекстное меню Удаленной установки Запустится Мастер создания задачи удаленной установки (рис. 5.35). Нажмите кнопку «Далее».

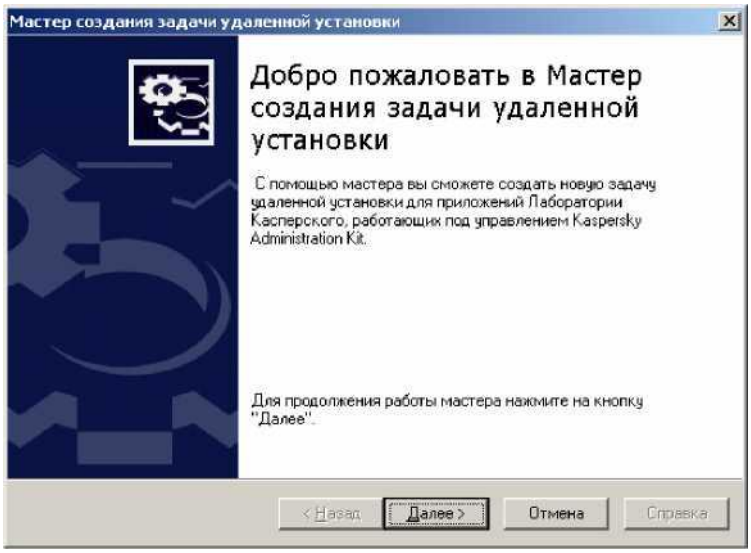

Рис. 5.35. Приветствие Мастера

На следующей странице Вам будет предложено задать имя создаваемой задачи удаленной установки (рис. 5.36). Нажмите кнопку «Далее».

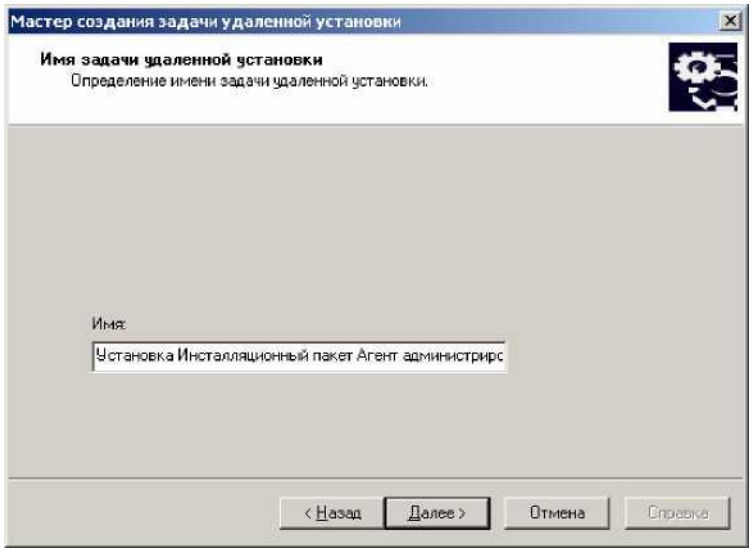

Рис. 5.36. Имя задачи удаленной установки На следующей странице Вам будет предложено выбрать метод удаленной установки (рис. 5.37). Выберите «Форсированная установка» и нажмите кнопку «Далее».

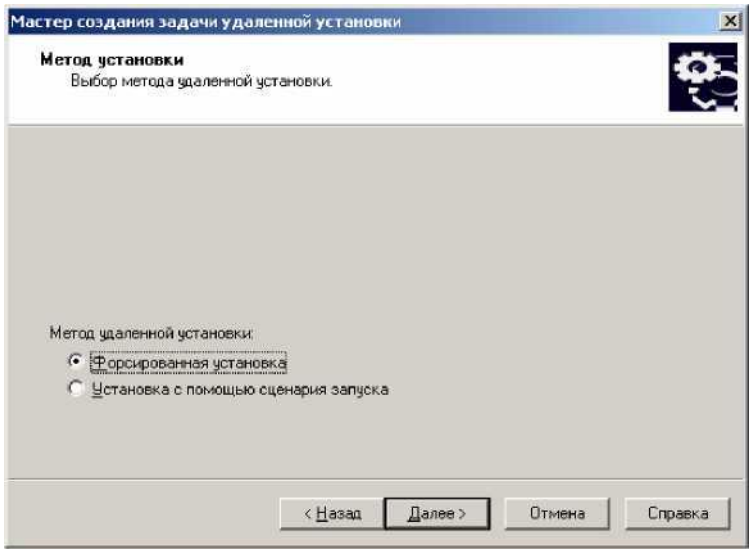

Рис. 5.37. Выбор метода установки

На следующей странице Вам будет предложено задать настройки выполнения задачи (рис. 5.38). Если на клиентском компьютере уже установлена старая версия Агента администрирования и Вам необходимо обязательно установить последнюю версию Агента администрирования, отключите параметр «Не устанавливать приложение, если оно уже установлено». Так как мы устанавливаем Агент администрирования на компьютер, где ещё не установлен Агент администрирования, включите параметр «Средствами Windowsиз папки общего доступа» и отключите параметр «С помощью Агента администрирования». Остальные параметры оставьте без изменения и нажмите кнопку «Далее».

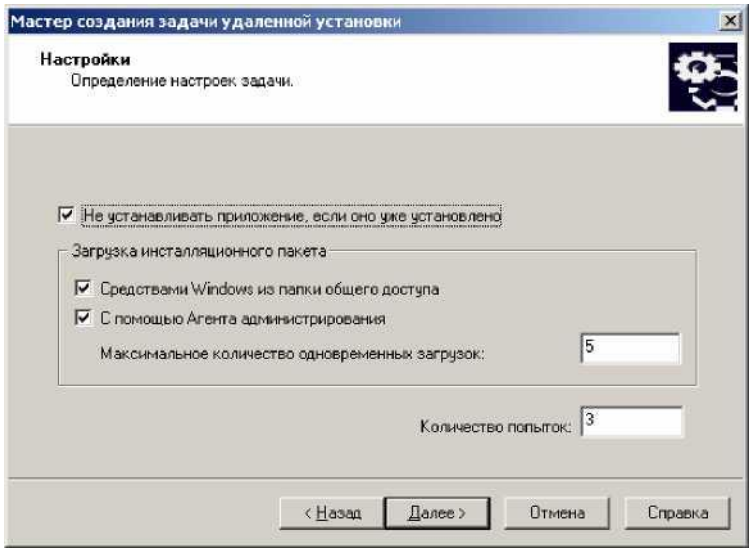

Рис. 5.38. Определение настроек задачи

На следующей странице Вам будет предложено определить способ выбора клиентских компьютеров, на которые будет установлен Агент администрирования (рис. 5.39). Выберите вариант «На основании данных, полученных в ходе опроса Windows-сети» и нажмите кнопку «Далее».

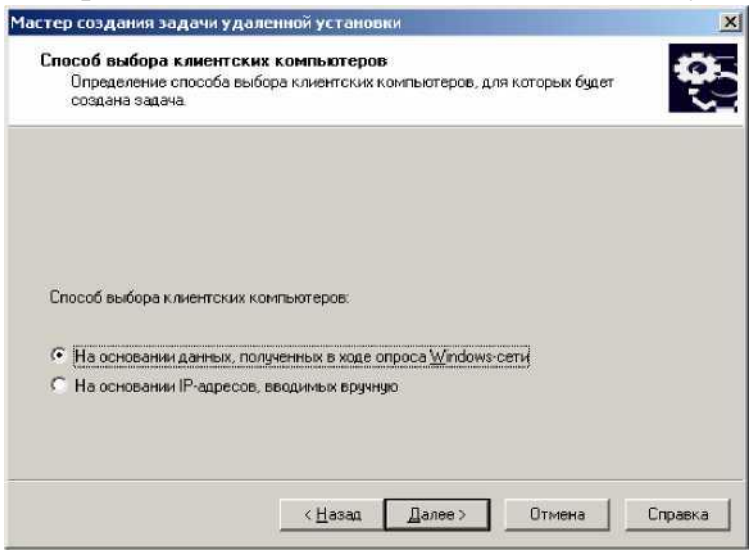

Рис. 5.39. Способ выбора клиентских компьютеров На следующей странице Вам будет предложено определить перечень клиентских компьютеров, на которые будет установлен Агент администрирования (рис. 5.40). Разверните раздел «Группы», отметьте компьютер «Client01» и нажмите кнопку «Далее».

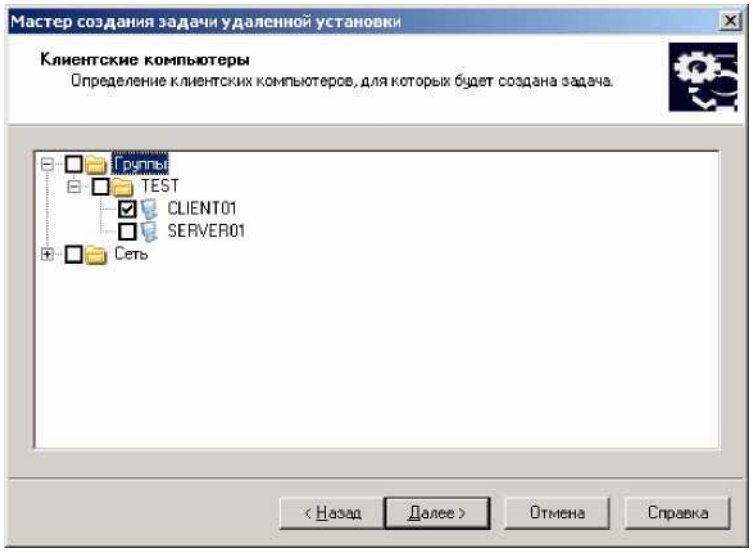

Рис. 5.40. Выбор клиентских компьютеров На следующей странице Вам будет предложено определить учетную запись для запуска создаваемой задачи (рис. 5.41). Если Вы выберите вариант «Учетная запись по умолчанию», то для запуска задачи удаленной установки будет использоваться учетная запись, под которой выполняется служба Сервера администрирования. Нажмите кнопку «Далее».

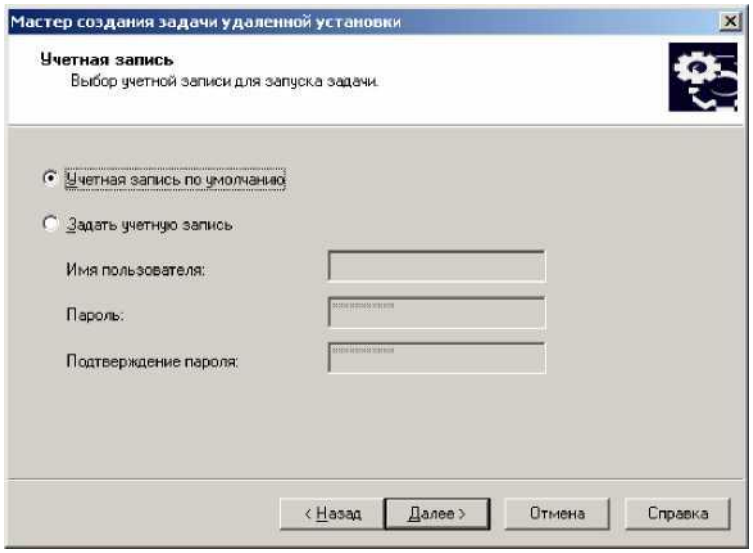

Рис. 5.41. Выбор учетной записи для запуска задачи На следующей странице Вам будет предложено определить расписание для запуска создаваемой задачи (рис. 5.42). На рисунке представлены доступные варианты. Выберите вариант «Немедленно» и нажмите кнопку «Далее».

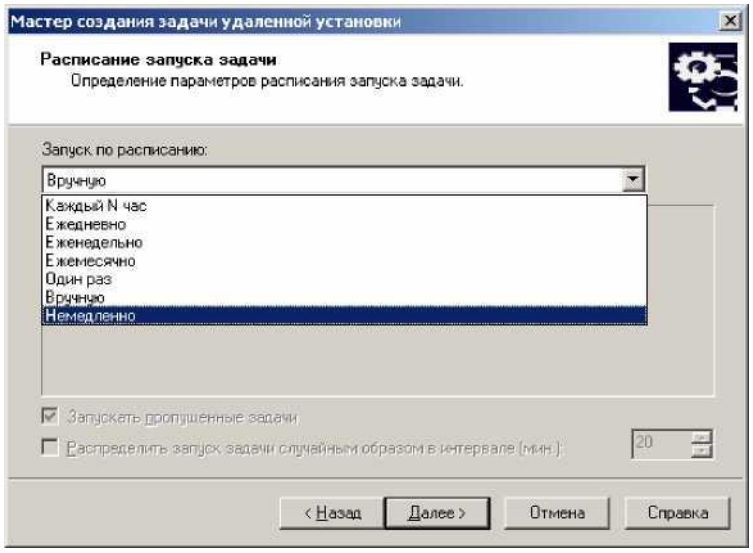

Рис. 5.42. Расписание запуска задачи На следующей странице (рис. 5.43) нажмите кнопку «Далее».

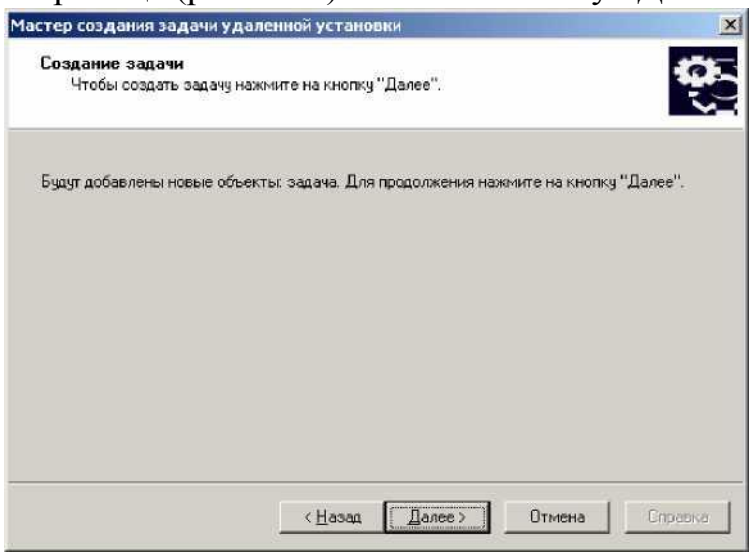

Рис. 5.43. Создание задачи

На следующей странице сообщается об успешности создания задачи «Установка Инсталляционный пакет Агент администрирования» (рис. 5.44). Для завершения работы Мастера нажмите кнопку «Готово».

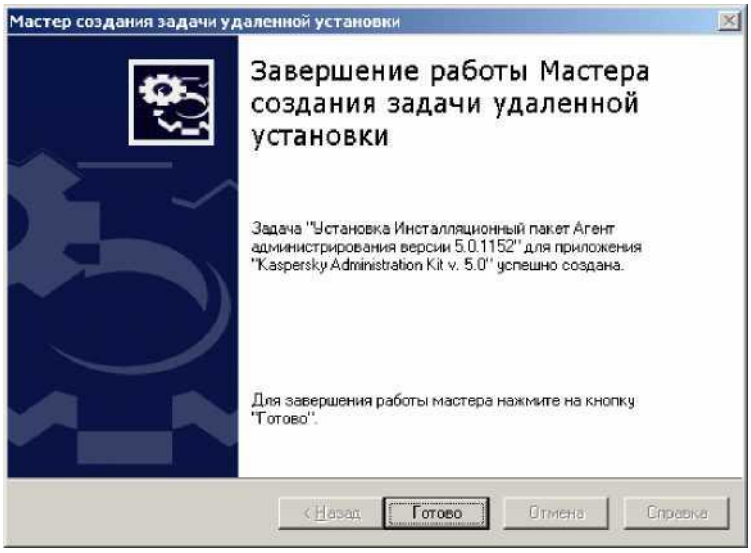

Рис. 5.44. Завершение работы Мастера

В левой части Консоли администрирования выберите «Глобальные задачи». В правой части окна Вы увидите созданную задачу «Установка Инсталляционный пакет Агент администрирования» (рис. 5.45). Во время выполнения задачи её значок отображается следующим образом: После успешного завершения задачи её значок изменится на &.

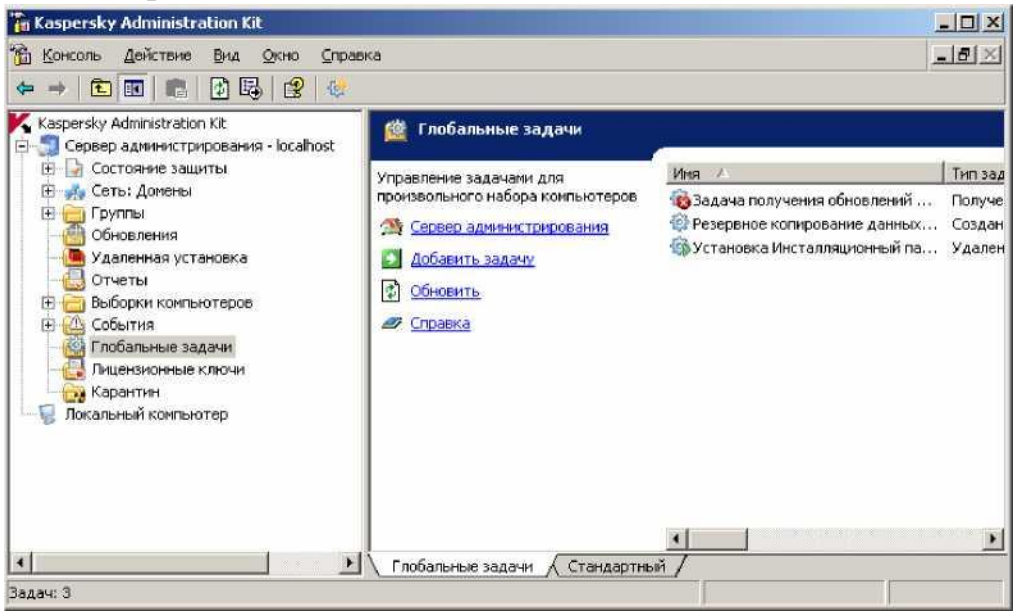

Рис. 5.45. Глобальные задачи

Вызовите контекстное меню этой задачи (см. рис. 5.46) и выполните команду «Результаты».

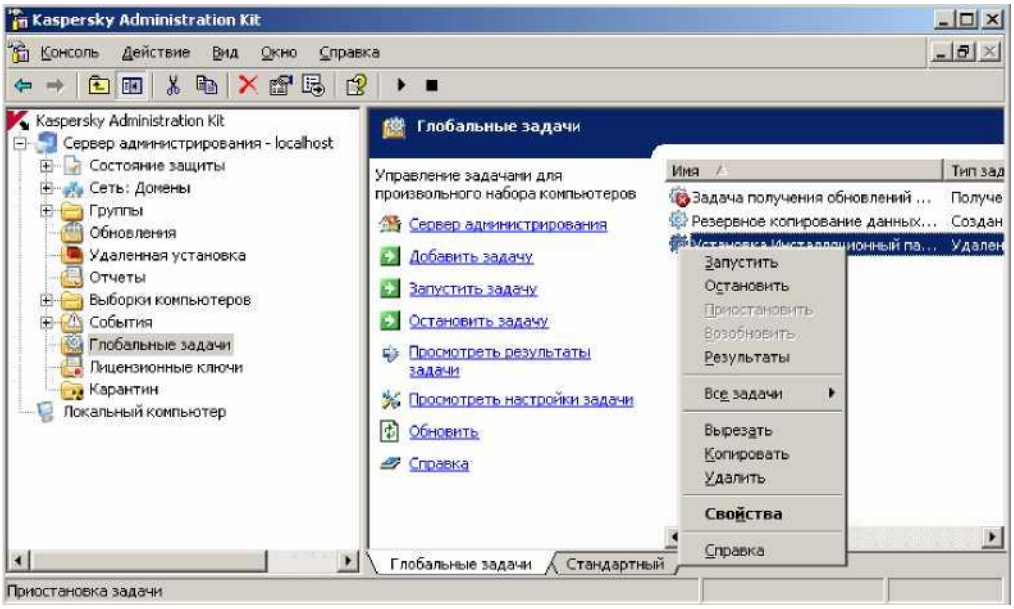

Рис. 5.46. Контекстное меню задачи

В левой части окна будут перечислены компьютеры, на которых выполнялась эта задача (см. рис. 5.47), а справа отображаются результаты выполнения задачи. Суммарную информацию о количестве компьютеров, где задача была успешна или не успешна, можно посмотреть, выполнив команду «Свойства» в контекстном меню задачи (см. рис. 5.48).

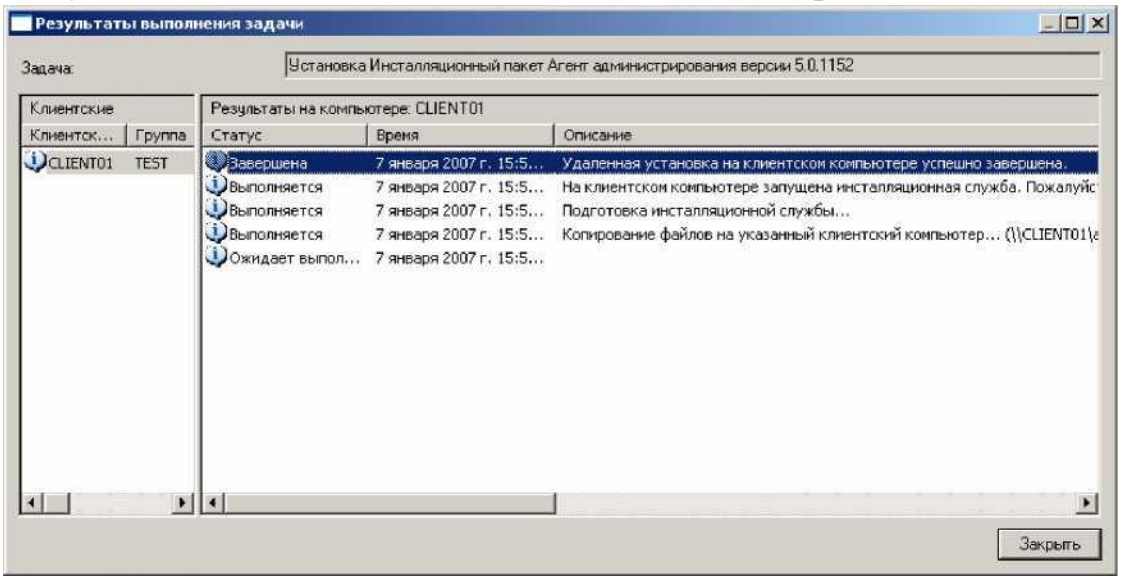

Рис. 5.47. Результаты выполнения задачи

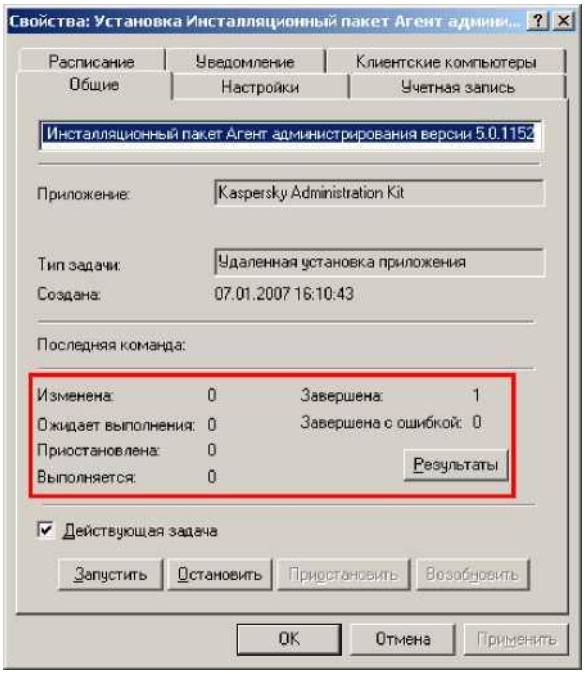

Рис. 5.48. Окно свойств задачи

5.3.8. Удаленная установка Антивируса Касперского® 5.0 для WindowsWorkstations

Удаленная установка Антивируса Касперского 5.0 для WindowsWorkstationаналогична удаленной установке Агента администрирования. Перед созданием соответствующей задачи, необходимо подготовить Инсталляционный пакет.

Откройте Консоль администрирования. Для этого зарегистрируйтесь на компьютере SERVER01 под учетной записью администратора домена или пользователя входящего в группу KLAdmins. Запустите программу KasperskyAdministrationKit. Для этого выполните «Пуск | Программы | KasperskyAdministrationKit| KasperskyAdministrationKit». Подключитесь к Серверу администрирования, нажав на значок + рядом с надписью «Сервер администрирования» (рис. 5.33).

В левой части Консоли администрирования вызовите контекстное меню узла «Удаленная установка» и выполните команду «Создать | Инсталляционный пакет» (рис. 5.49).

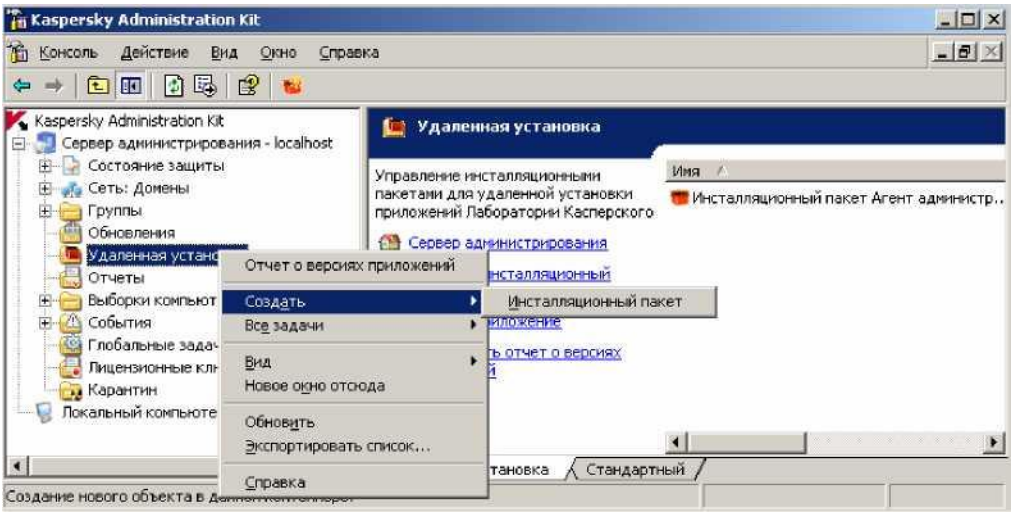

Рис. 5.49. Контекстное меню Удаленной установки Запустится Мастер создания инсталляционного пакета (рис. 5.50). Нажмите кнопку «Далее».

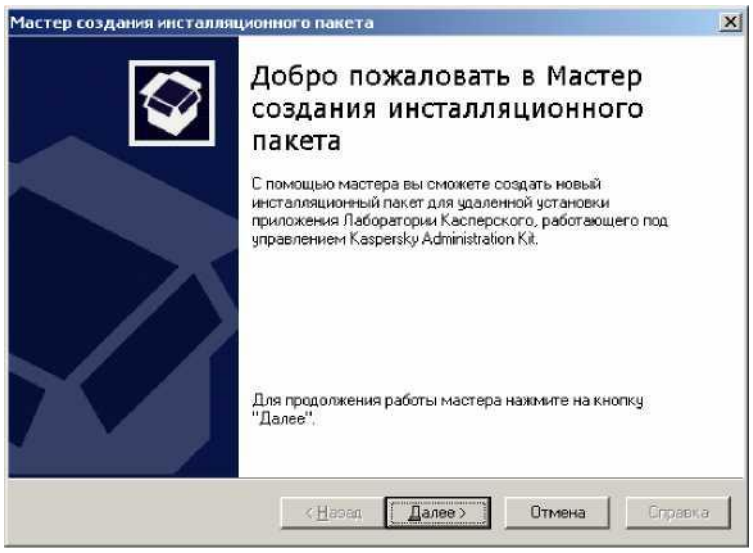

Рис. 5.50. Мастер создания инсталляционного пакета На следующей странице Вам будет предложено задать имя создаваемого инсталляционного пакета (рис. 5.51). Введите имя (например, «Инсталляционный пакет Антивирус Касперского для WindowsWorkstation») и нажмите кнопку «Далее».

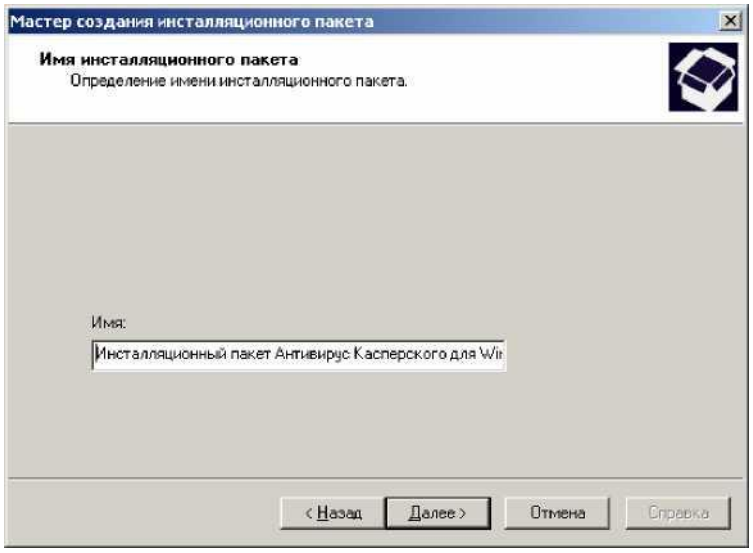

Рис. 5.51. Имя инсталляционного пакета

На следующей странице Вам будет предложено выбрать дистрибутив приложения для установки (рис. 5.52). Выберите «Создать инсталляционный пакет для приложения Лаборатории Касперского». С помощью кнопки «Обзор» укажите расположение распакованного дистрибутива Антивируса Касперского для WindowsWorkstation. Точнее необходимо указать файл с расширением .kpdиз состава дистрибутива (см. рис. 5.53). После указания нужного файла, нажмите кнопку «Далее».

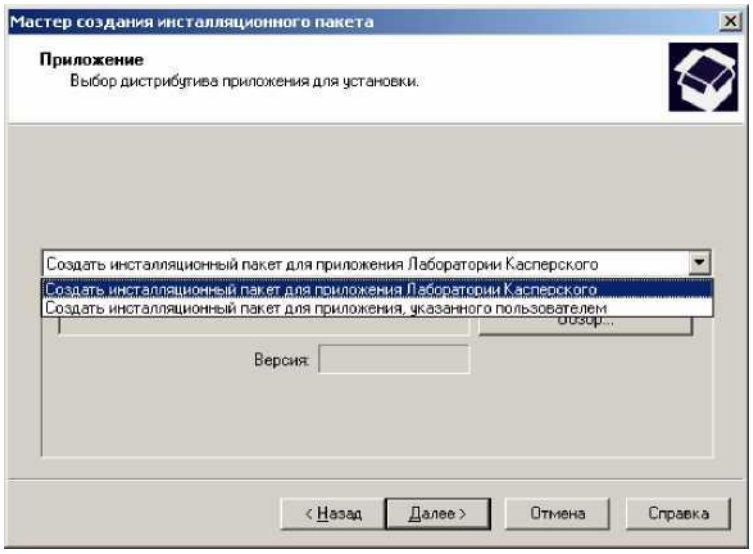

Рис. 5.52. Выбор дистрибутива продукта

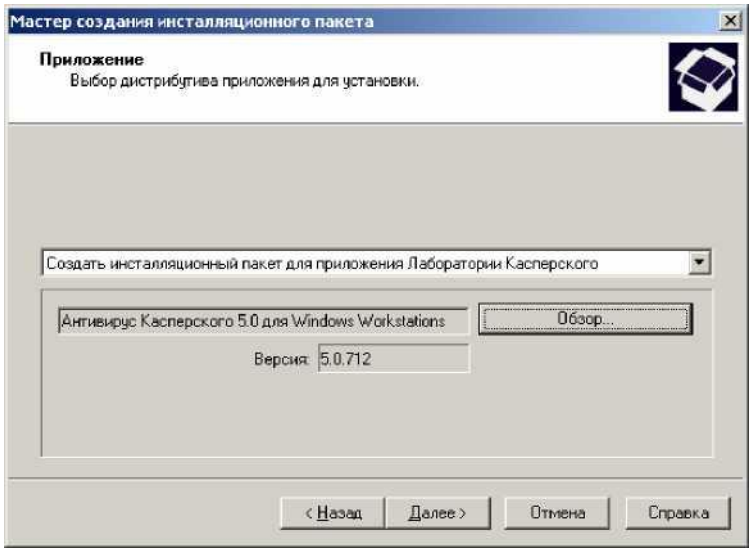

Рис. 5.53. После указания файла .kpd

На следующей странице Вам будет предложено указать лицензионный ключ для устанавливаемого продукта (рис. 5.54). С помощью кнопки «Обзор...» укажите нужный файл и нажмите кнопку «Далее».

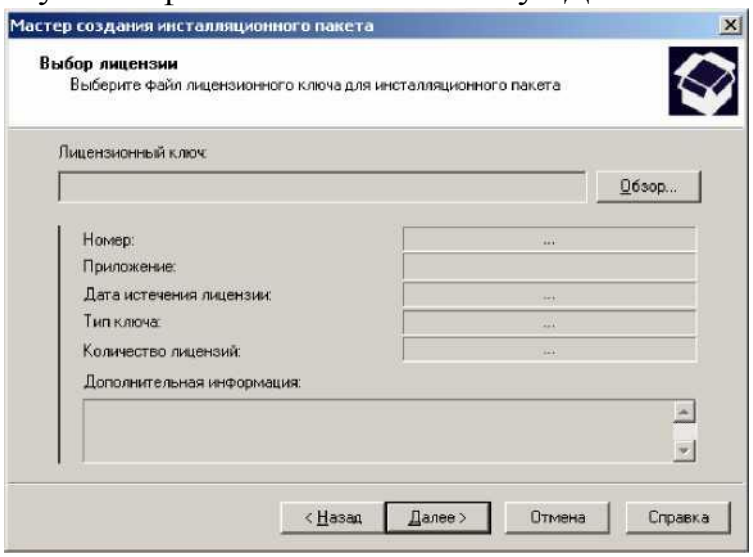

Рис. 5.54. Выбор лицензии

Здесь необходимо отметить один существенный момент. Все создаваемые инсталляционные пакеты хранятся в папке общего доступа, имя которой было задано при установке Сервера администрирования (см. рис. 5.15 в п. 5.3.4). Лицензионный ключ, который Вы указываете при создании инсталляционного пакета, также располагается в этой папке. В документации к KaspersкyAdministrationKit[7] не дается каких либо рекомендаций о том, как предотвратить утечку лицензионного ключа из этого источника пользователями организации. Можно предложить следующее решение этой проблемы. При создании инсталляционного пакета не указывать лицензионный ключ. А для установки лицензионного ключа создать отдельную задачу, которую выполнять после завершения установки антивирусного продукта на компьютер.

На следующей странице (рис. 5.55) нажмите кнопку «Далее».

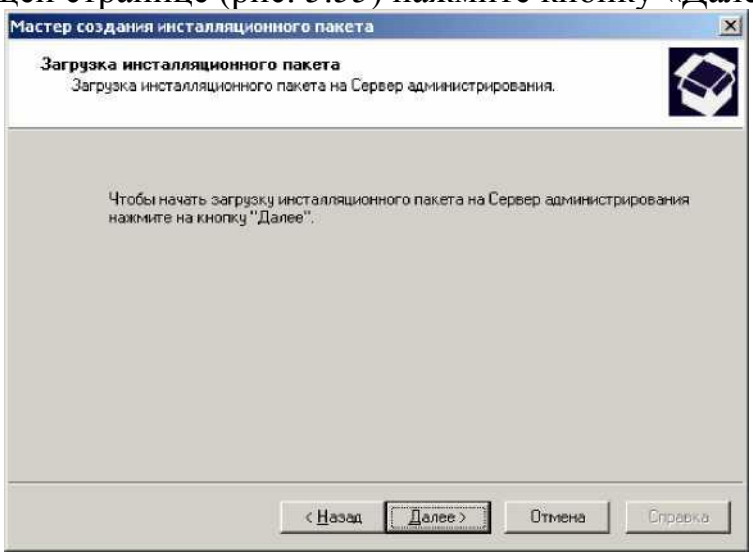

Рис. 5.55. Загрузка инсталляционного пакета Если во время загрузки инсталляционного пакета появится предупреждение, показанное на рис. 5.56, нажмите кнопку «Открыть» и загрузка будет продолжена.

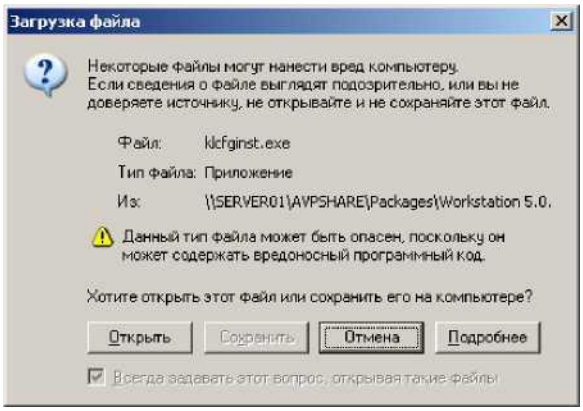

Рис. 5.56. Предупреждение ОС

На следующей странице сообщается об успешности создания инсталляционного пакета (рис. 5.57). Для завершения работы Мастера нажмите кнопку «Готово».

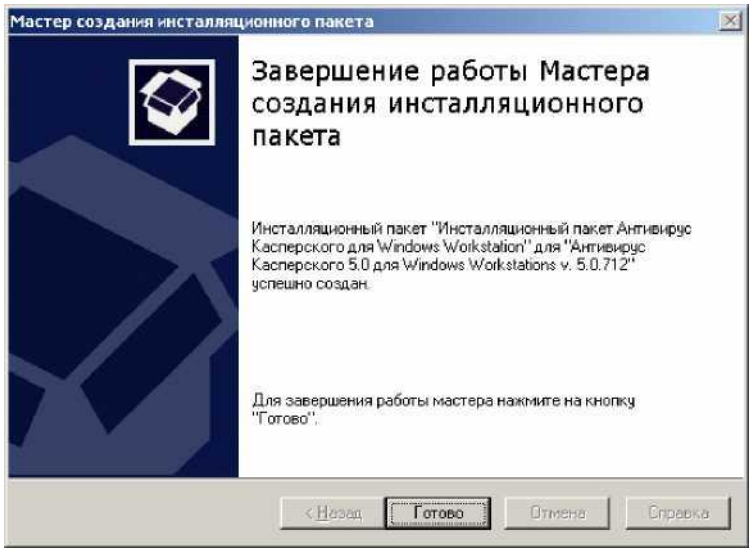

Рис. 5.57. Завершение работы Мастера

Прежде чем сформировать задачу удаленной установки на основе созданного пакета, Вам может потребоваться изменить некоторые свойства созданного инсталляционного пакета. Для этого, с помощью контекстного меню инсталляционного пакета, выполните команду «Свойства». Основные страницы свойств пакета представлены на рис. 5.58-5.60. Все параметры интуитивно понятны, поэтому не будем на них останавливаться.

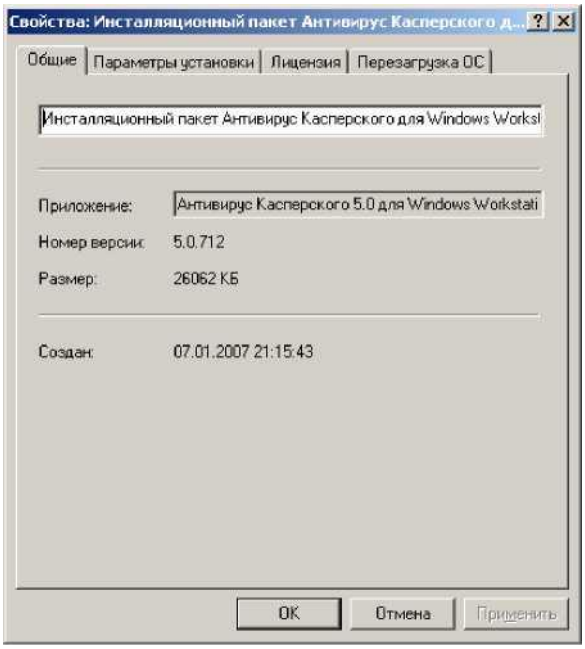

Рис. 5.58. Страница Общие

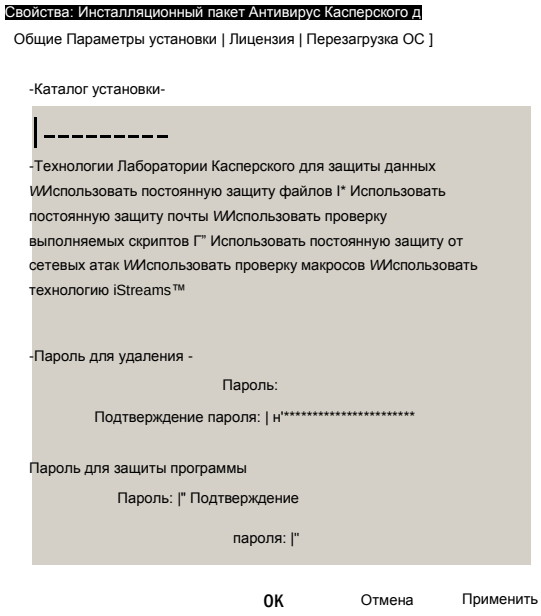

Рис. 5.59. Страница Параметры установки

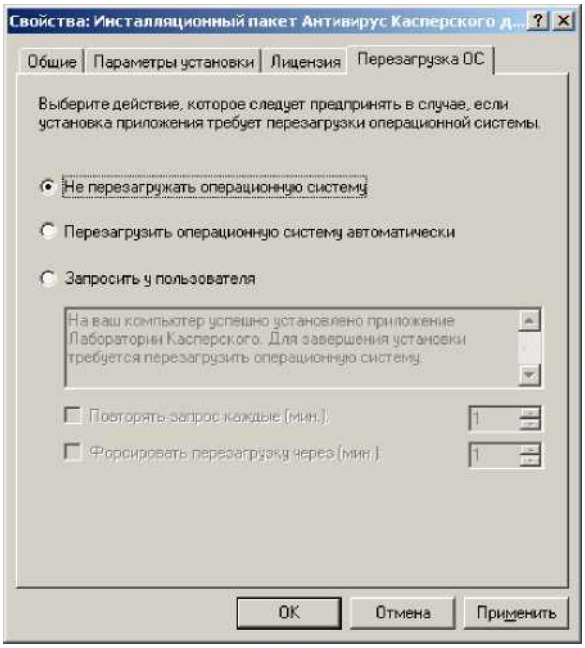

Рис. 5.60. Страница Перезагрузка ОС

Создание задачи удаленной установки на основе созданного нами инсталляционного пакета аналогично описанию в п. 5.3.7. Поэтому не будем останавливаться на этом. Не забудьте проверить результаты выполнения Задачи удаленной установки. На рис. 5.61 представлен возможный результат.

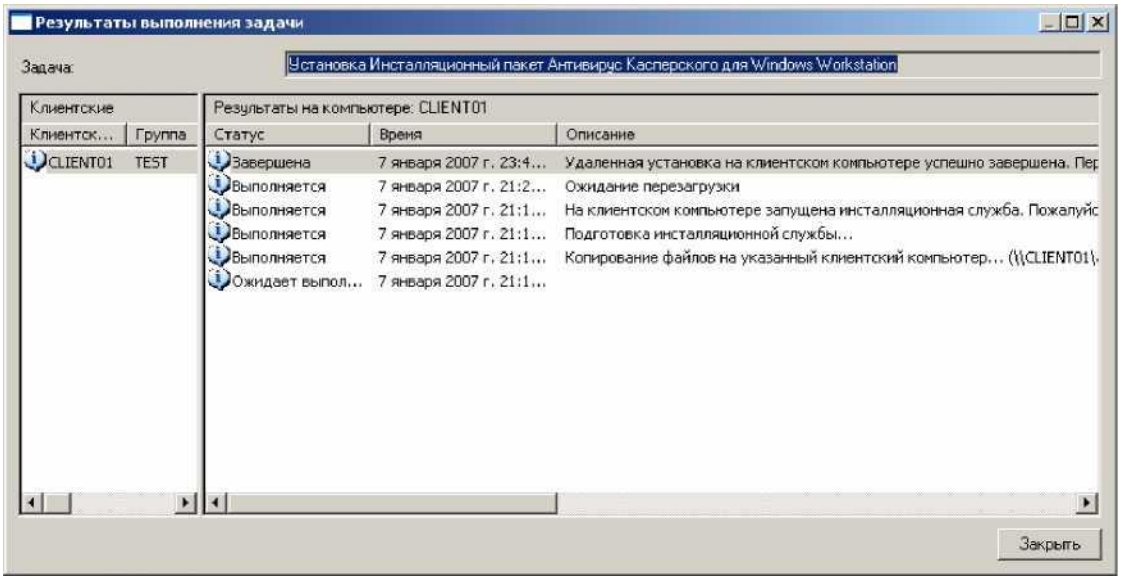

Рис. 5.61. Результаты выполнения задачи

5.3.9. Удаленная установка Антивируса Касперского® 5.0 для WindowsFileServers

Удаленная установка Антивируса Касперского для WindowsFileServersне сильно отличается от удаленной установки Антивируса Касперского для WindowsWorkstations. Во-первых, необходимо создать соответствующий Инсталляционный пакет (аналогично описанию в п. 5.3.8). Во-вторых, необходимо сформировать и выполнить глобальную Задачу установки этого пакета на Server01. Не забудьте проверить успешность выполнения этой задачи. На рис. 5.62 представлен возможный результат.

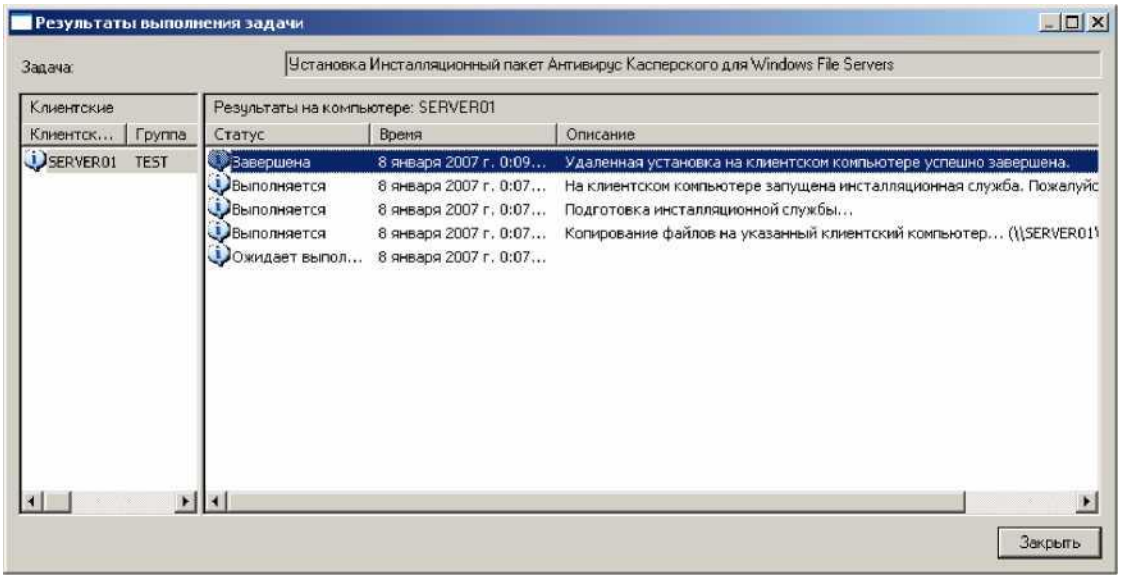

Рис. 5.62. Результаты выполнения задачи

5.4. Настройка получения антивирусных обновлений

При использовании Сервера администрирования, рекомендуется использовать следующую схему получения обновлений клиентскими станциями:

1) Сервер администрирования получает обновления из Интернета.

2) Клиентские приложения получают обновления с сервера администрирования.

Рассмотрим эти задачи более подробно.

5.4.1. Получение обновлений Сервером администрирования

Задача получения обновлений Сервером администрирования (см. рис. 5.63-2) создается Мастером первоначальной настройки (см. п. 5.3.5) и находится в узле «Глобальные задачи» верхнего уровня дерева консоли (см. рис. 5.63-1). С помощью контекстного меню Вы можете просмотреть свойства этой задачи и, в случае необходимости, изменить их. На рис. 5.64 представлена закладка «Настройки» окна свойств этой задачи. На рис. 5.65 представлены возможные источники обновления.

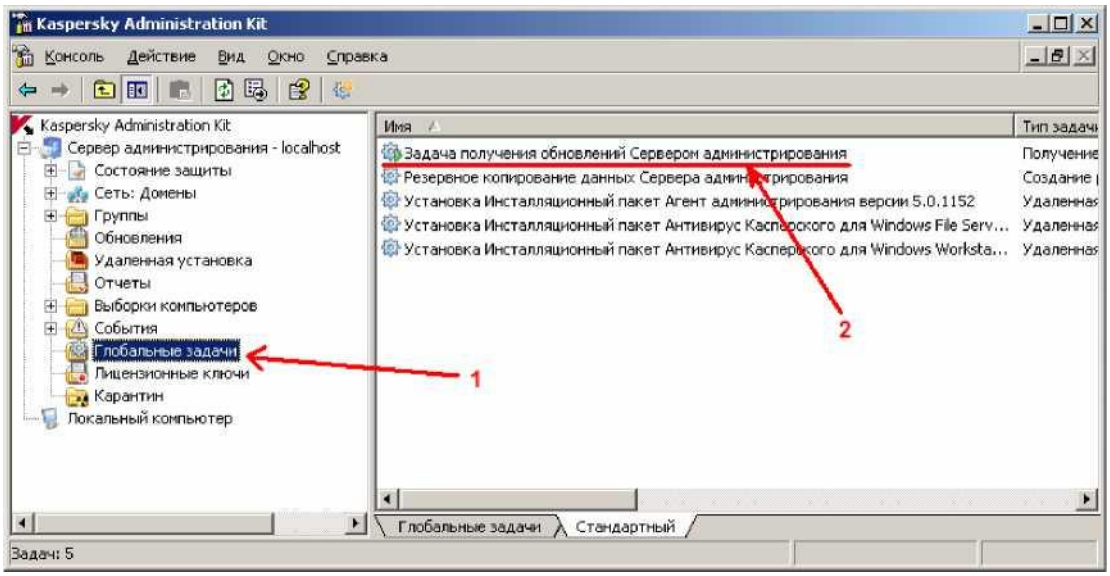

Рис. 5.63. Задача получения обновлений Сервером администрирования

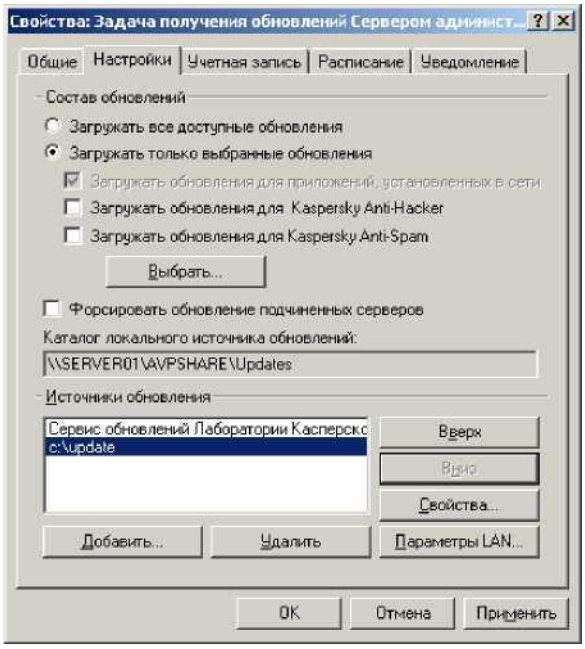

Рис. 5.64. Страница Настройки

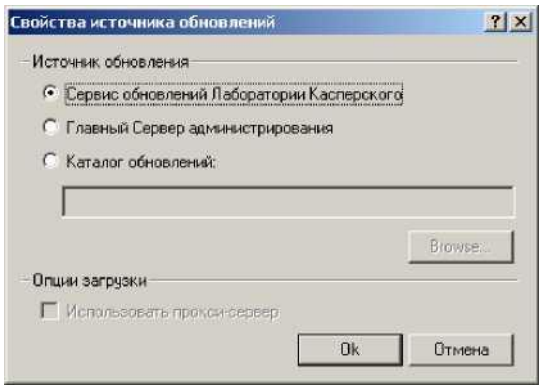

Рис. 5.65. Источники обновления

Обновление антивирусных баз на сайтах Лаборатории Касперского производится каждый час [9]. Лаборатория Касперского рекомендует проводить обновление антивирусных баз также как можно чаще и незамедлительно устанавливать все критические обновления программных модулей [7].

Как и для других задач, проверить правильность выполнения задачи обновления можно, выполнив команду «Результаты» из контекстного меню задачи (рис. 5.66). Кроме того, в дереве консоли в узле Обновления (см. рис. 5.67-1) появится информация о загруженных на Сервер администрирования обновлениях (см. рис. 5.67-2). Физически, получаемые обновления располагаются в папке общего доступа, имя которой было задано при установке Сервера администрирования (см. рис. 5.15 в п. 5.3.4) [7].

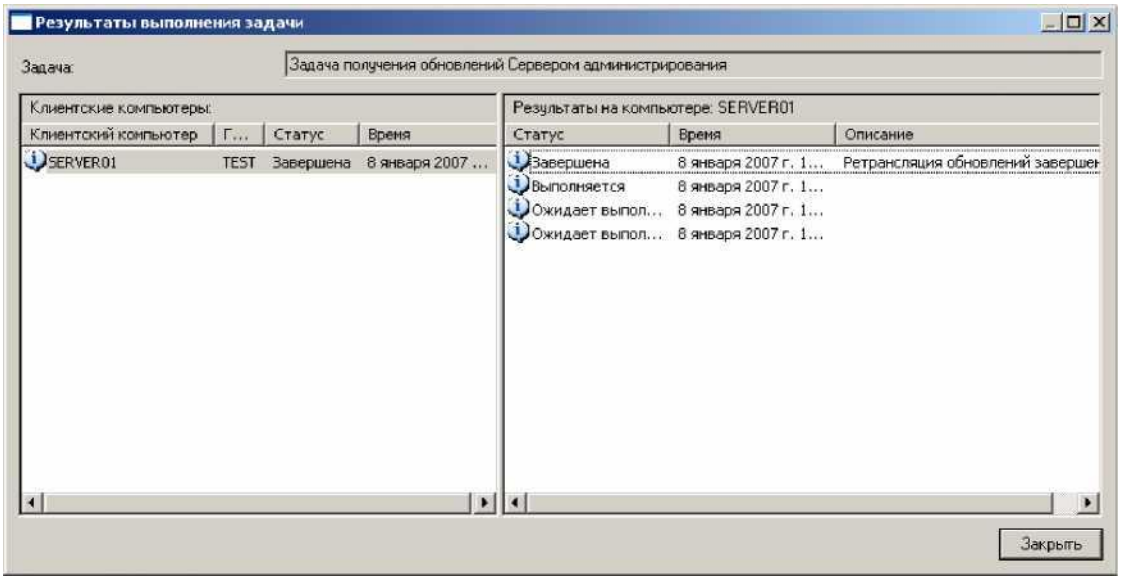

Рис. 5.66. Результаты выполнения задачи

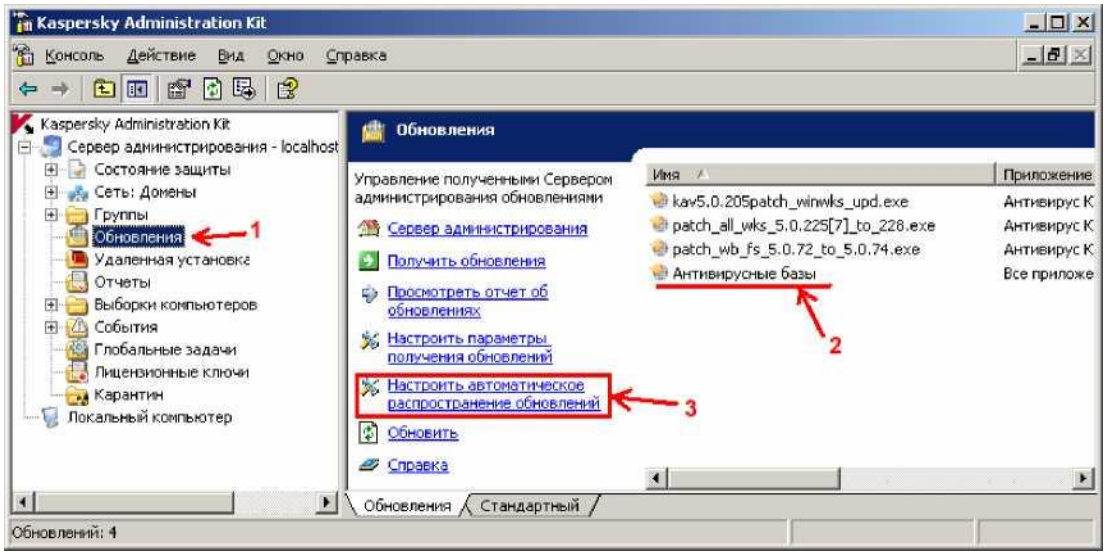

Рис. 5.67. Узел Обновления

5.4.2. Получение обновлений Антивирусными продуктами

Задача получения обновлений клиентскими станциями с установленным Антивирусом Касперского для WindowsWorkstation(см. рис. 5.68-2) создается Мастером первоначальной настройки (см. п. 5.3.5) и находится в папке «Групповые задачи» узла «Группы» верхнего уровня дерева консоли (см. рис. 5.68-1). С помощью контекстного меню Вы можете просмотреть свойства этой задачи и, в случае необходимости, изменить их.

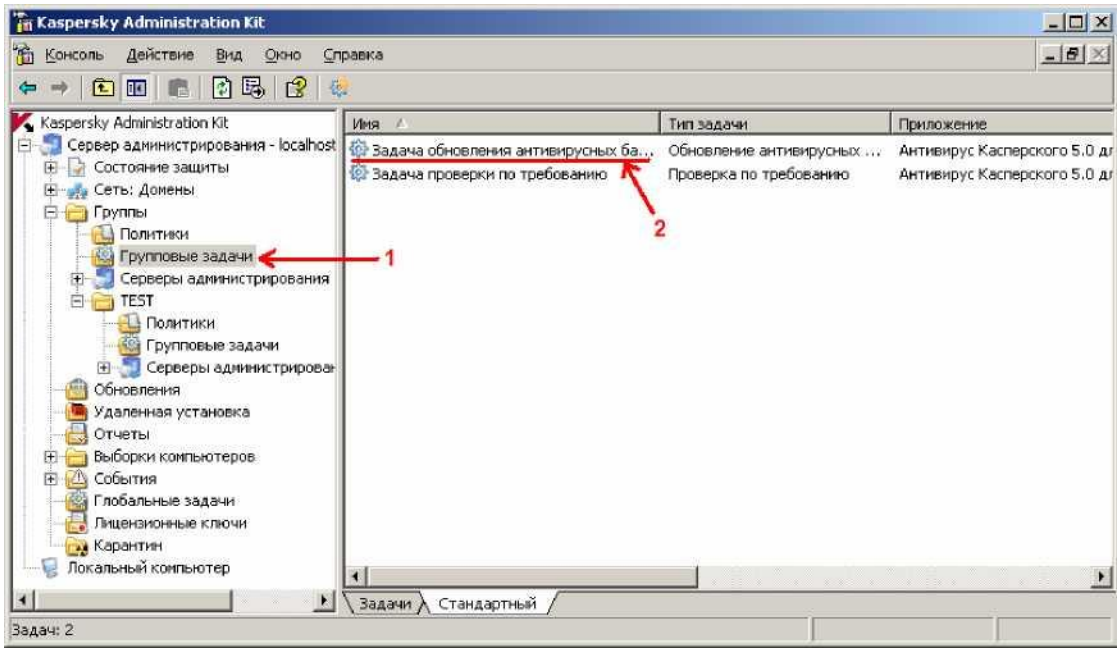

Рис. 5.68. Задача обновления антивирусных баз На рис. 5.69 представлена закладка «Настройки» окна свойств этой задачи. Если в Вашей организации обновление клиентских станций будет осуществляться только с Сервера администрирования, то в этом окне можно отключить источник обновления «Серверы обновлений Лаборатории Касперского».

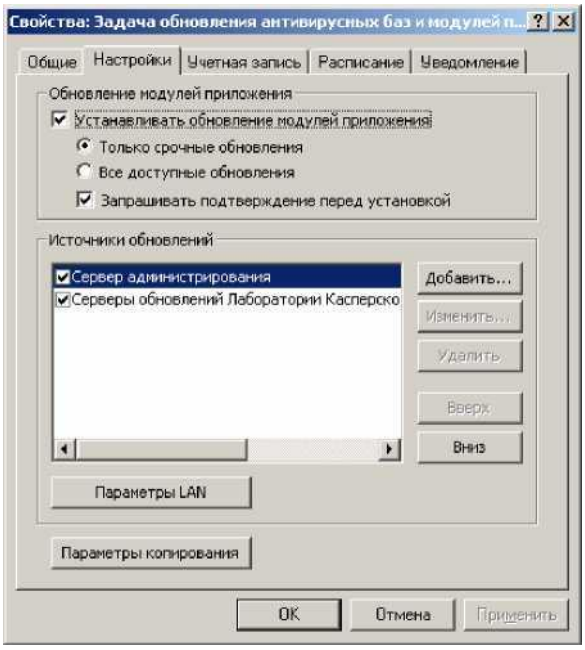

Рис. 5.69. Страница Настройки

Так как в нашем примере у нас существуют не только Антивирусы Касперского® для WindowsWorkstation, но и Антивирусы Касперского® для WindowsFileServers, то необходимо создать аналогичную задачу обновления антивирусных баз для приложения Антивирус Касперского® для WindowsFileServers. Для этого в контекстном меню папки «Групповые

задачи» узла «Группы» верхнего уровня дерева консоли (см. рис. 5.68-1) выполнить команду «Создать | Задачу». Запустится Мастер создания задачи (рис. 5.70). Нажмите кнопку «Далее».

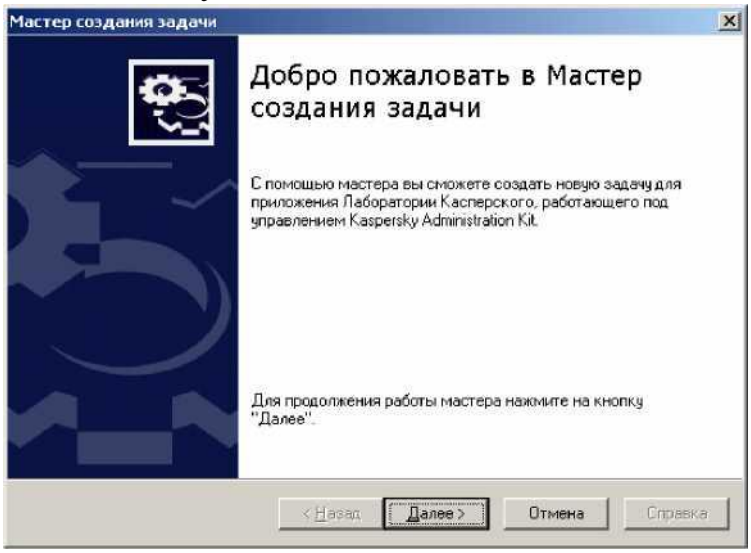

Рис. 5.70. Приветствие Мастера

На следующей странице Вам будет предложено задать имя создаваемой задачи (рис. 5.71). Введите имя (например, «Обновление WindowsFile Servers») и нажмите кнопку «Далее».

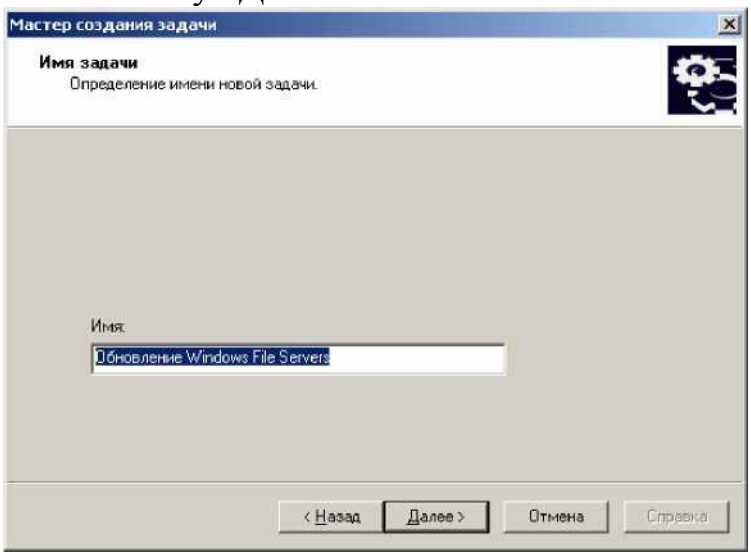

Рис. 5.71. Имя задачи

На следующей странице Вам будет предложено указать приложение, для которого будут создаваться задача и указать её тип (рис. 5.72). В разделе «Приложение» выберите «Антивирус Касперского 5.0 для WindowsFileServers», а в разделе «Тип задачи» укажите «Обновление антивирусных баз и модулей приложения» и нажмите кнопку «Далее».

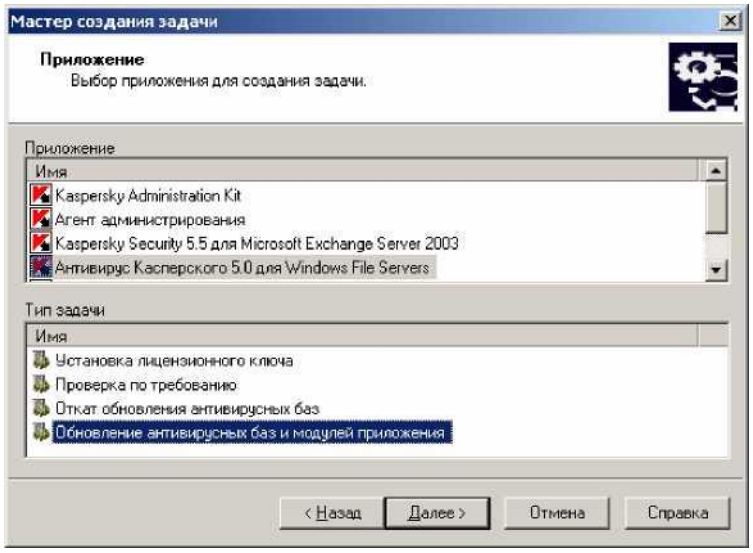

Рис. 5.72. Выбор приложения и типа задачи На следующей странице Вам будет предложено выбрать источник обновления (рис. 5.73). Выберите «Сервер администрирования» и нажмите кнопку «Далее».

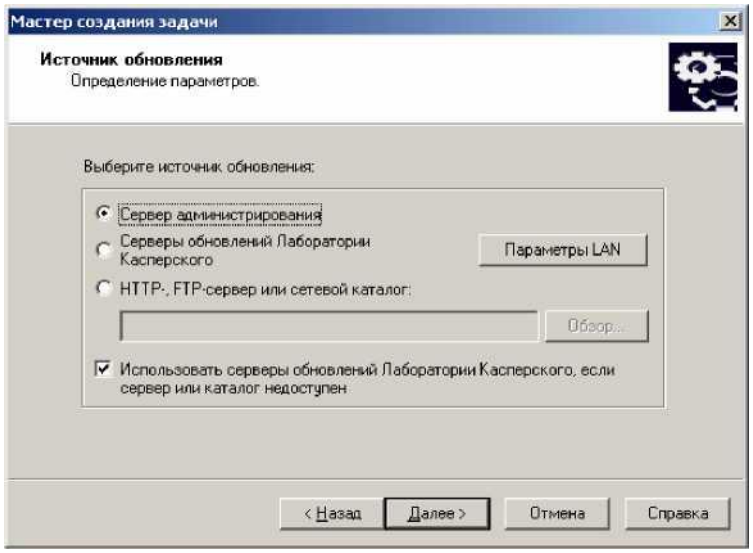

Рис. 5.73. Выбор источника обновления

На следующей странице Вам будет предложено определить параметры обновления антивирусных баз и обновлений модулей приложения (рис. 5.74). Укажите нужные Вам параметры и нажмите кнопку «Далее».

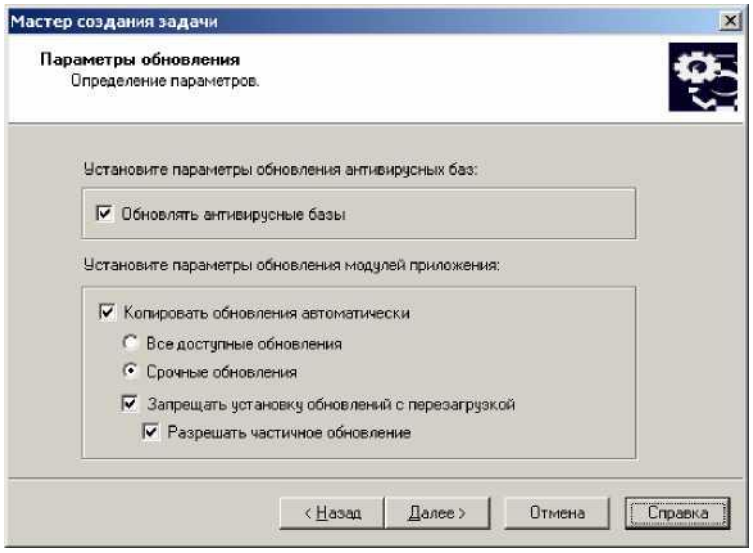

Рис. 5.74. Параметры обновления

На следующей странице Вам будет предложено определить, будут ли получаемые обновления копироваться в локальный источник на клиентском компьютере (рис. 5.75). Нажмите кнопку «Далее».

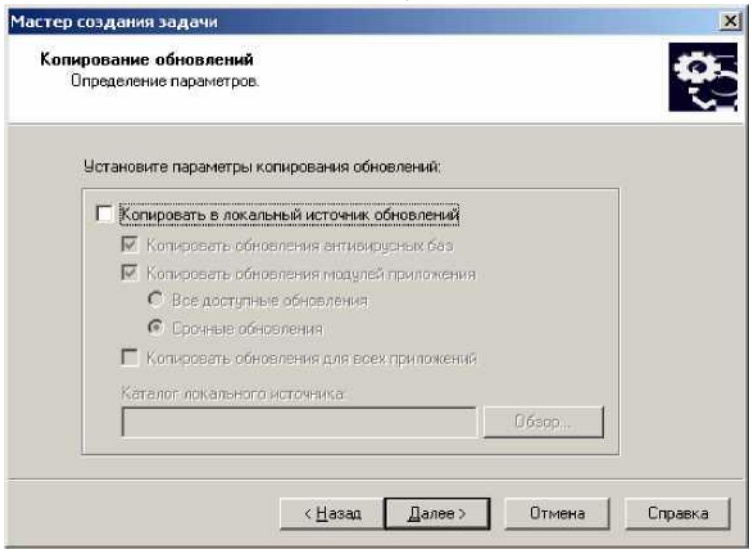

Рис. 5.75. Копирование обновлений

На следующей странице Вам будет предложено определить учетную запись для запуска создаваемой задачи (рис. 5.76). Нажмите кнопку «Далее».

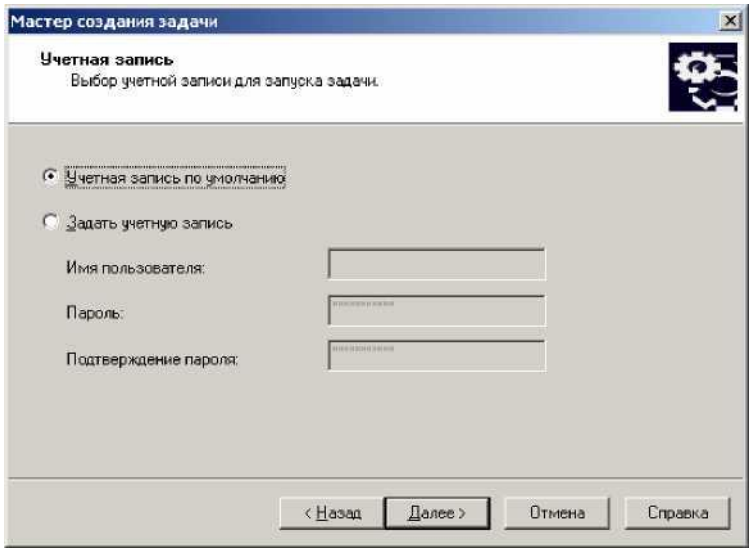

Рис. 5.76. Выбор учетной записи

На следующей странице Вам будет предложено определить расписание для запуска создаваемой задачи (рис. 5.77). На рисунке представлены доступные варианты. Выберите нужный Вам вариант и нажмите кнопку «Далее».

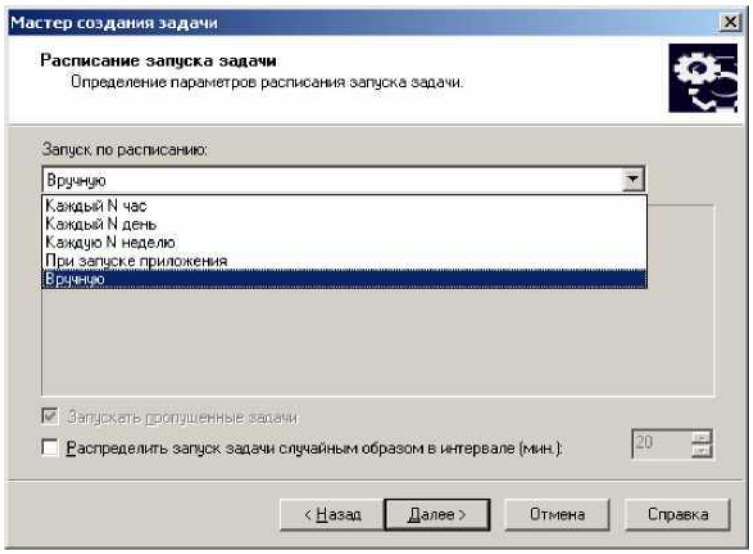

Рис. 5.77. Расписание запуска задачи На следующей странице (рис. 5.78) нажмите кнопку «Далее».

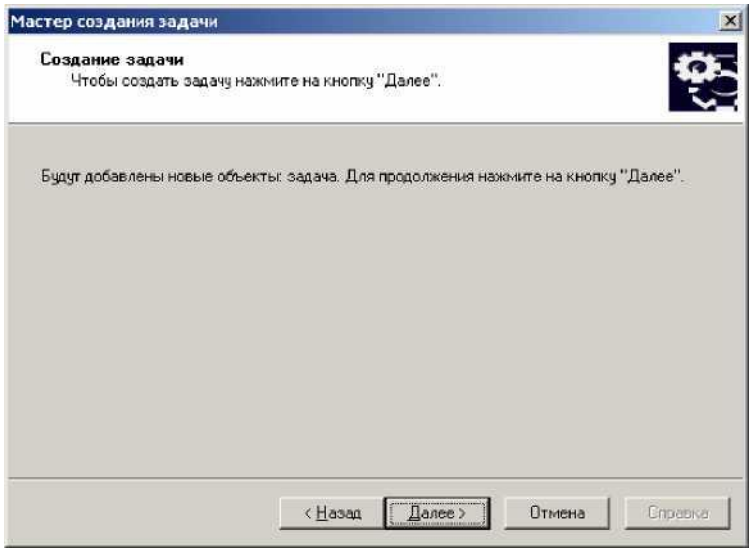

Рис. 5.78. Создание задачи

На следующей странице сообщается об успешности создания задачи (рис. 5.79). Для завершения работы Мастера нажмите кнопку «Готово».

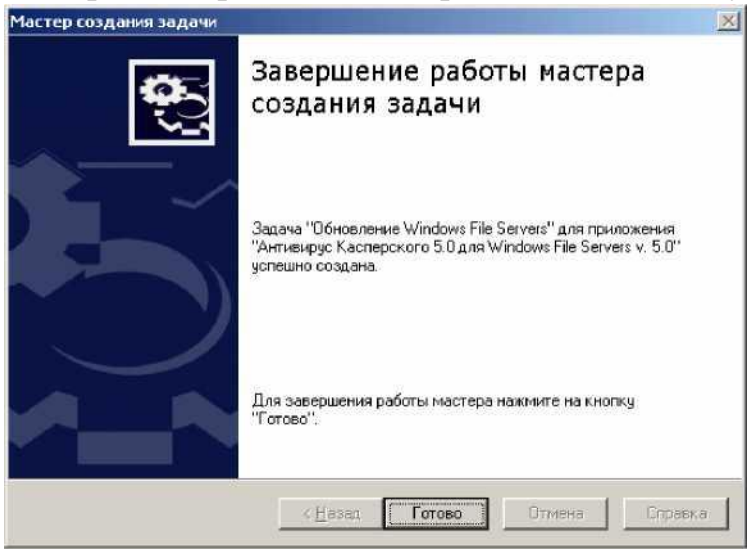

Рис. 5.79. Завершение работы Мастера

В контекстном меню созданной задачи выполните команду «Запустить». Дождитесь завершения задачи (её значок изменится с ^ на Ф) и, с помощью команды контекстного меню «Результаты», откройте окно результатов (рис. 5.80).

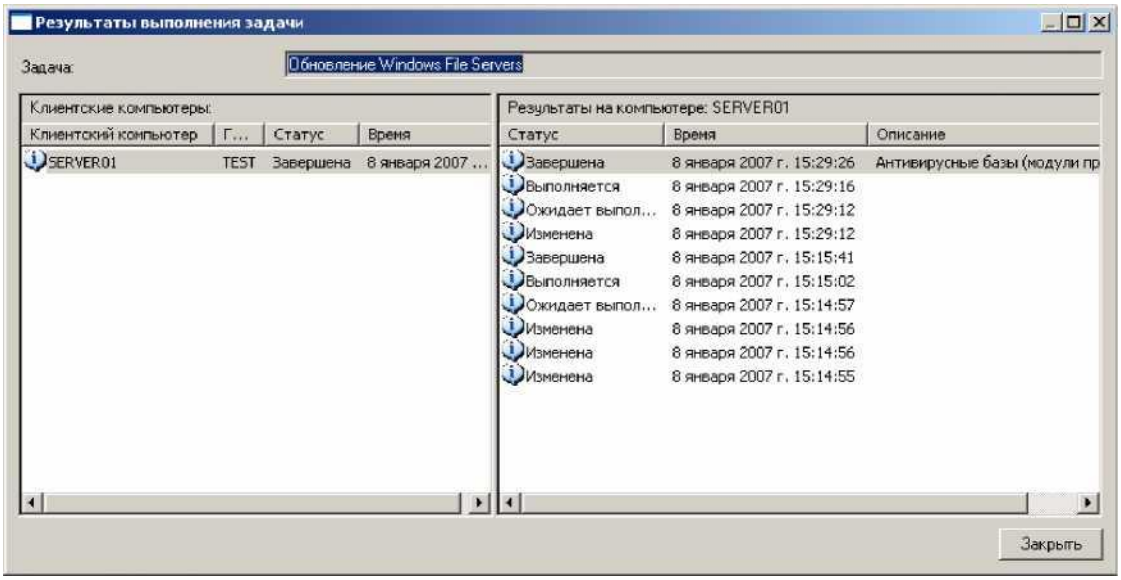

Рис. 5.80. Результаты выполнения задачи

5.4.3. Автоматическое распространение обновлений

Кроме описанного выше способа создания отдельных задач выполнения обновления антивирусных баз на клиентских компьютерах, существует механизм так называемого «Автоматического распространения обновлений». Для его включения необходимо в дереве Консоли администрирования открыть свойства узла «Обновления» и включить соответствующий параметр (рис. 5.81).

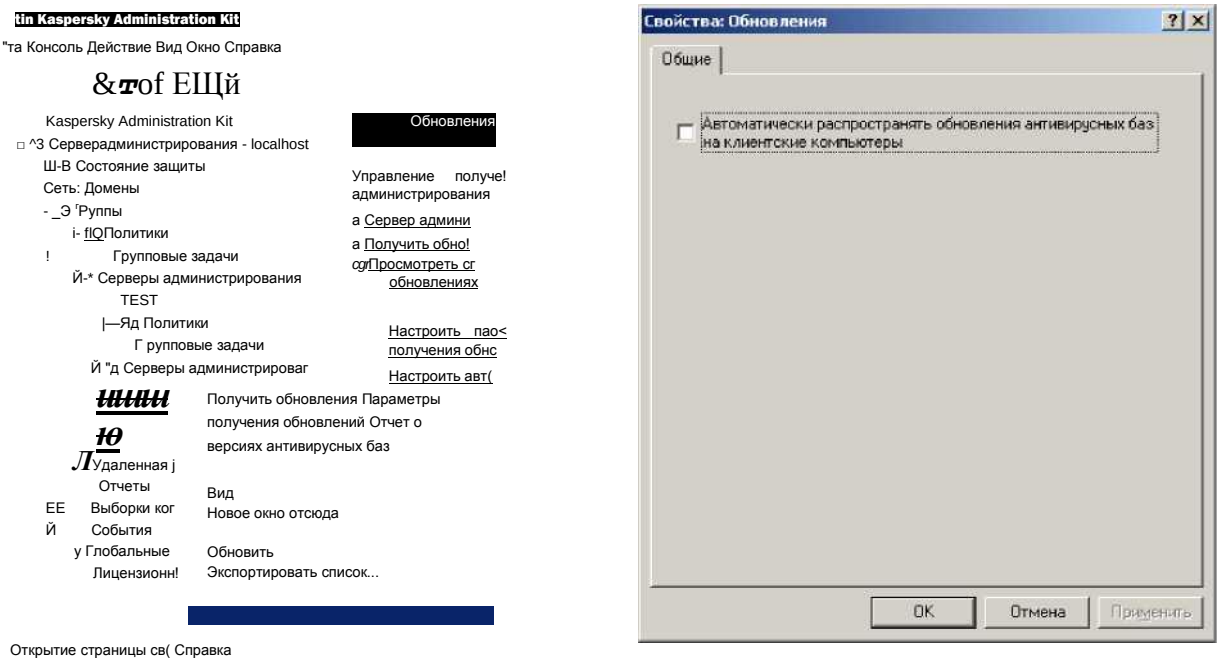

Рис. 5.81. Свойства узла Обновления

В результате этого Сервер администрирования автоматически создаст групповые задачи верхнего уровня иерархии (см. рис. 5.82-1) для всех приложений компании, установленных на клиентских компьютерах логиче-

ской сети. Эти задачи отображаются в папке «Групповые задачи» узла «Группы» (см. рис. 5.82-2), и удалить их можно, только сняв флажок «Автоматически распространять обновления антивирусных баз на клиентские компьютеры» (рис. 5.81). При получении обновлений Сервер администрирования будет запускать эти задачи автоматически. Параметры задач автоматического обновления можно редактировать аналогично любой другой задаче обновления [7].

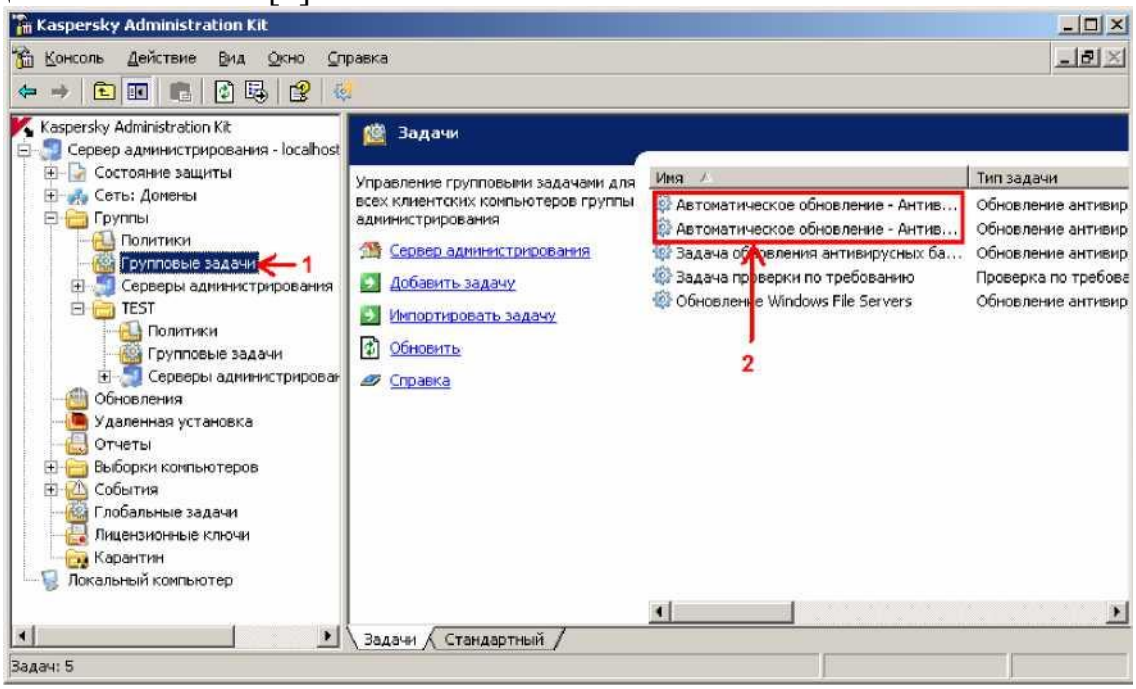

Рис. 5.82. Задачи автоматического распространения обновлений

5.5. Настройка параметров уведомлений о событиях

Ранее уже было сказано, что Сервер администрирования позволяет отправлять уведомления о возникающих событиях (например, обнаружение вируса и т.п.) по электронной почте или средствами NETSEND. Рассмотрим настройки, регулирующие этот процесс.

Во-первых, настройки по умолчанию, определяющие адреса электронной почты, SMTP-сервера и перечень компьютеров для отправки уведомлений средствами NETSENDзадаются в свойствах Сервера администрирования (см. рис. 5.83, 5.84).

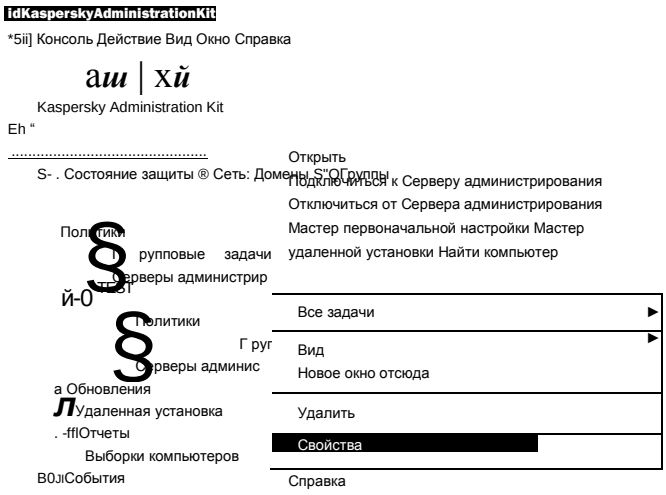

Рис. 5.83. Контекстное меню Сервера администрирования

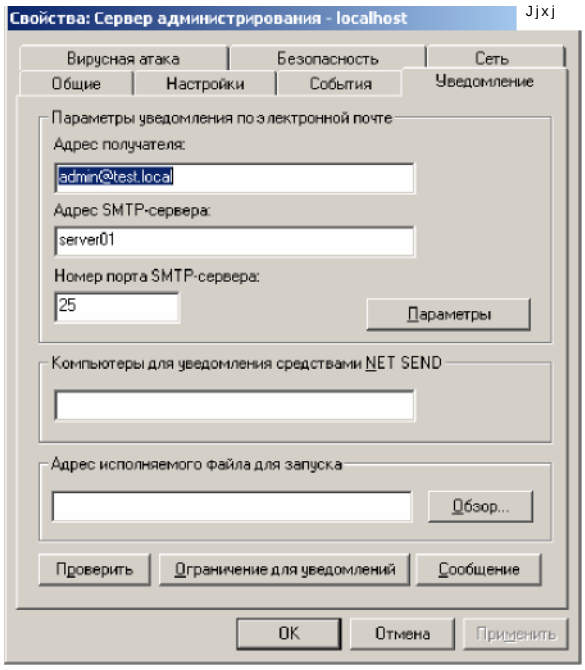

Рис. 5.84. Свойства Сервера администрирования Во-вторых, сам перечень событий для каждого антивирусного приложения задается в соответствующих политиках. Например, политика Антивируса Касперского для WindowsWorkstations(созданная Мастером первоначальной настройки (см. п. 5.3.5)), располагается в папке «Политики» узла «Группы» (см. рис. 5.85).

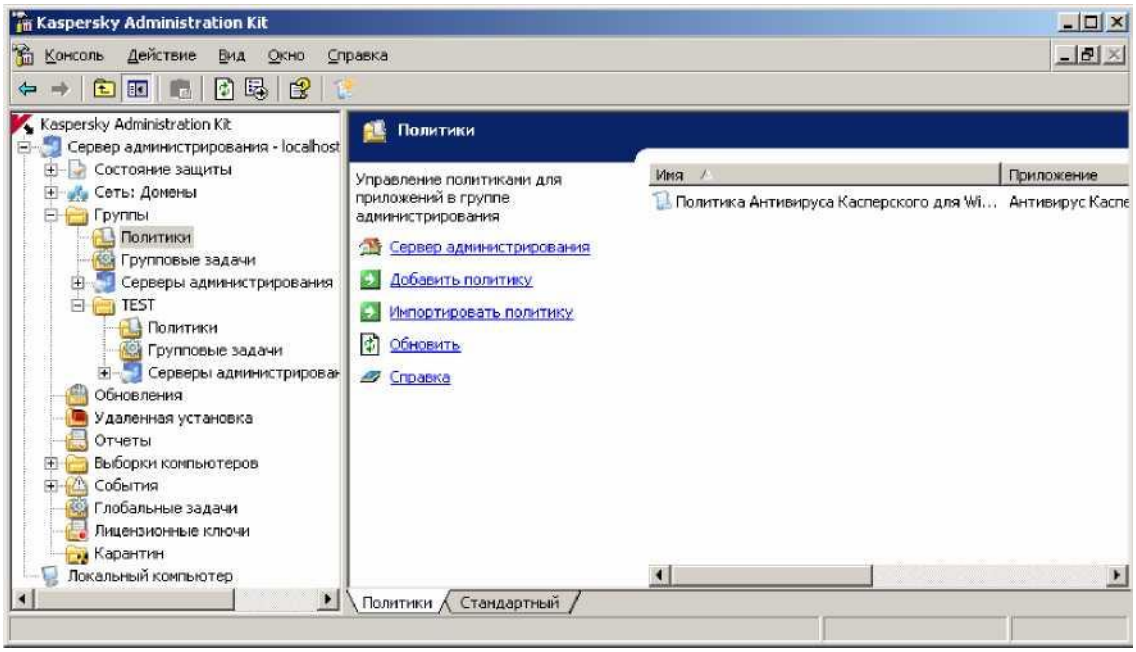

Рис. 5.85. Расположение глобальных политик Перечень событий и варианты реагирования располагаются в политике на закладке «События» (рис. 5.86). Выберите нужные Вам события для каждого уровня важности и включите параметр «Уведомлением по электронной почте». Если Вы хотите задать адрес электронной почты отличный от заданного по умолчанию в свойствах Сервера администрирования (см. рис. 5.84), нажмите кнопку «Параметры» (рис. 5.86).

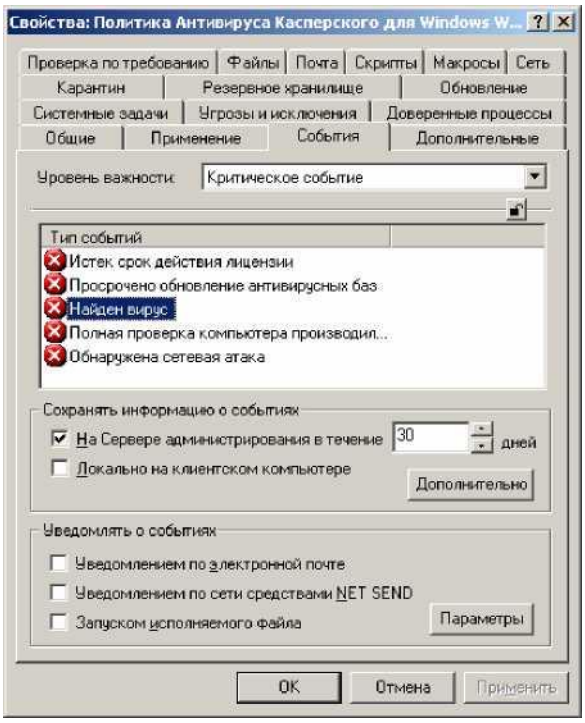

Рис. 5.86. Закладка События

Если Вам необходимо получать уведомления о событиях появляющихся в работе Антивируса Касперского для WindowsFileServers, Вам необ-

ходимо создать политику для этого приложения и задать в ней настройки интересующих Вас событий. Создание такой политики не создаст у Вас затруднений. Подробнее о Политиках Вы можете прочитать в [7].

5.6. Получение отчетов

По умолчанию, большинство событий записываются в журнале событий Сервера администрирования (см. рис. 5.86, параметр «Сохранять информацию о событиях на сервере администрирования»). Используя эти данные, Вы можете создавать отчеты по заранее сформированным шаблонам [7].

Шаблоны отчетов расположены в узле «Отчеты» в Консоли администрирования. На рис. 5.87 представлено 8 стандартных отчетов.

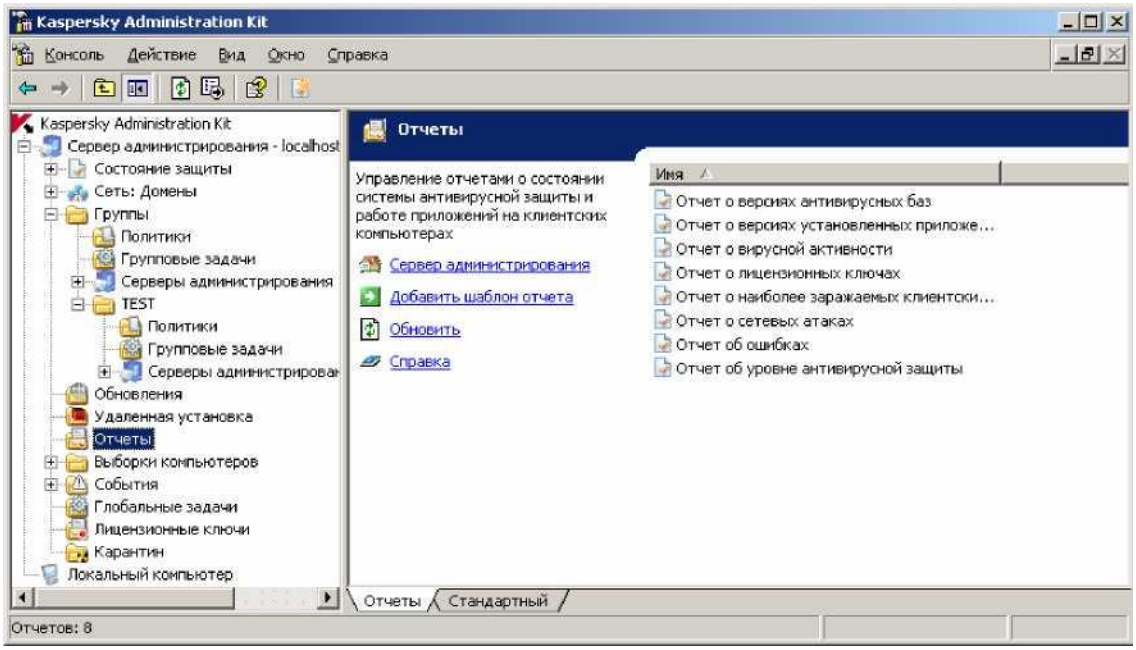

Рис. 5.87. Узел Отчеты

Подробнее о параметрах создания отчетов Вы можете прочитать в документации [7]. Обратите внимание, что существует возможность создать задачу автоматической рассылки отчетов по электронной почте (см. рис. 5.89). Например, очень удобно получать каждый день информацию о версиях антивирусных баз установленных на серверах в Вашей организации.

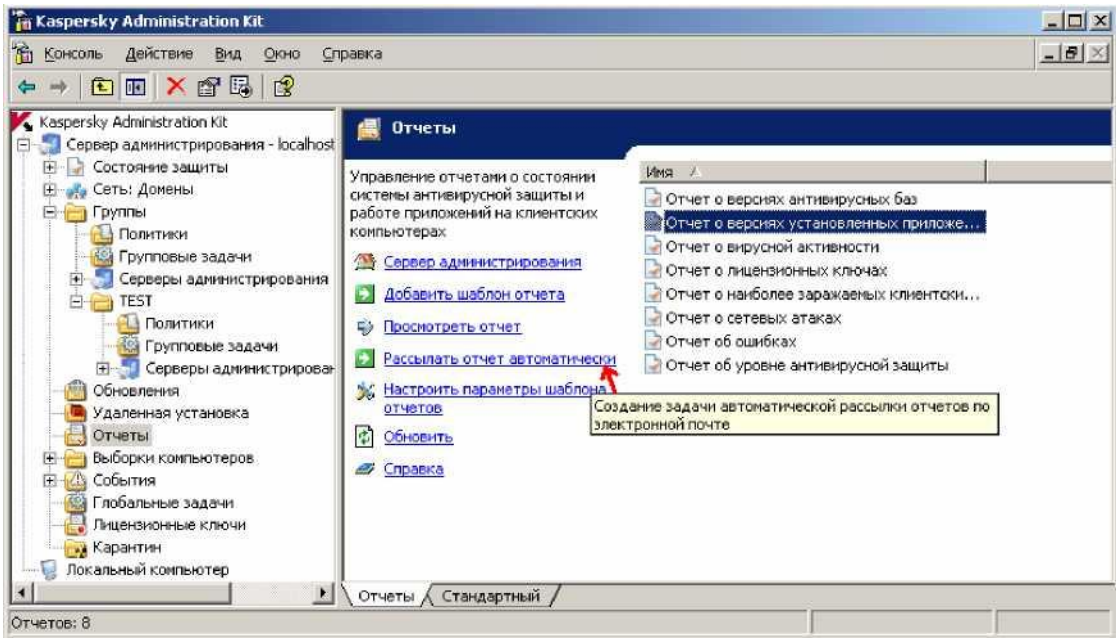

Рис. 5.89. Узел Отчеты

5.7. Резервное копирование данных Сервера администрирования

Периодическое создание резервной копии данных Сервера администрирования KasperskyAdministrationKitявляется одной из важных задач обеспечения отказоустойчивости антивирусной защиты в организации. В случае выхода из строя сервера, на котором функционирует Сервер администрирования, на его восстановление может потребоваться очень много времени, если у Вас нет резервной копии. Конечно, Вы можете использовать стандартное резервное копирований файлов и баз данных, но есть более удобный способ сделать резервную копию этих данных.

Во-первых, существует утилита командной строки `klbackup`, которую можно использовать для этих целей. Подробнее о ней можно прочитать в документации [7].

Во-вторых, в узле «Глобальные задачи» уже существует соответствующая задача (рис. 5.90). Её только необходимо настроить: задать расписание для её выполнения, определить папку для хранения резервных копий и пароль для шифрования сертификата Сервера администрирования (см. рис. 5.91).

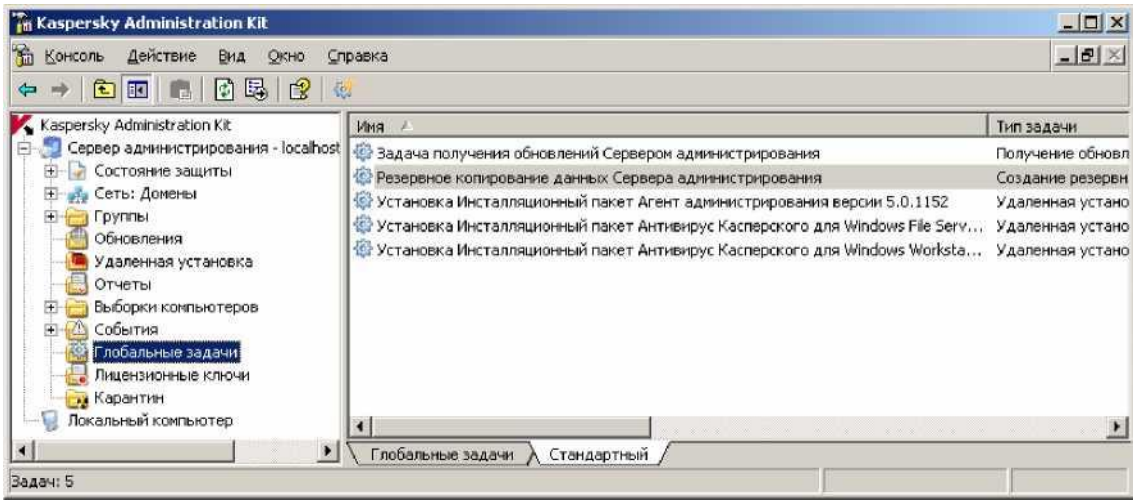

Рис. 5.90. Задача «Резервное копирование...»

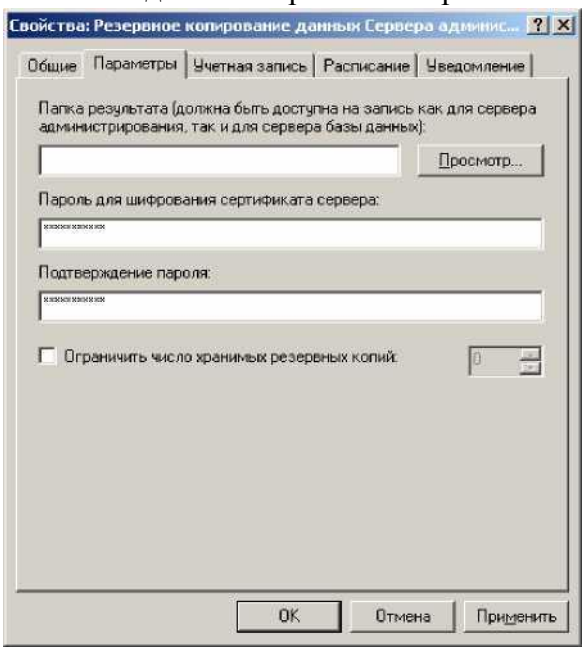

Рис. 5.91. Закладка «Параметры»

5.8. **Лабораторная работа № 1.** Подготовительная настройка сетевой инфраструктуры

В этой лабораторной работе Вы добавите на компьютер server01 роль «Почтовый сервер (POP3, SMTP)», создадите три почтовых ящика (`admin@test.local`, `user01@test.local` и `user02@test.local`) и настроите почтовых клиентов для работы с созданными ящиками. Первый почтовый ящик будет использоваться для получения уведомлений от Сервера администрирования, остальные для демонстрации возможностей Антивируса Касперского.

Предварительные требования

Для выполнения данной работы необходимо наличие двух (можно виртуальных) компьютеров объединенных в домен test.local. Один компьютер

- serverOlпод управлением WindowsServer2003. Учетная запись администратора домена «Administrator», пароль «P@ssw0rd». Другой компьютер - clientOlпод управлением WindowsXP.

Лабораторная работа 1 выполняется на компьютерах server01 (установка роли «Почтовый сервер», настройка почтового клиента для ящика admin@test.local)и client01 (настройка почтовых клиентов для ящиков user01@test.localи user02@test.local).

5.8.1. Упражнение 1. Установка почтовой службы

Вы добавите на компьютер server01 роль «Почтовый сервер (POP3, SMTP)».

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. запустите «Мастер настройки сервера». Для этого выполните команду «Пуск | Программы | Администрирование | Управление данным сервером».
3. В появившемся окне нажмите «Добавить или удалить роль».
4. На странице «Предварительные шаги» нажмите кнопку «Далее».
5. На странице «Роль сервера» выберите роль «Почтовый сервер (POP3, SMTP)» и нажмите кнопку «Далее».
6. На странице «Настройка службы POP3» укажите «Метод проверки подлинности:» - «Интегрированные с ActiveDirectory» и «Имя домена электронной почты:» - «test.local» (без кавычек). Нажмите кнопку «Далее».
7. На странице «Сводка выбранных параметров» нажмите «Далее».
8. После завершения установки, нажмите кнопку «Готово».

5.8.2. Упражнение 2. Создание почтовых ящиков

Вы создадите три почтовых ящика (admin@test.local, user01@test.localи user02@test.local)и соответствующие им доменные учетные записи.

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. Откройте окно управления почтовым сервером. Для этого выполните «Пуск | Программы | Администрирование | Служба POP3».
3. В левой части окна разверните пункт SERVER01 и вызовите контекстное меню для почтового сервера test.local. Выполните команду «Создать | Почтовый ящик...».
4. В окне «Добавление почтового ящик» в поле «Имя почтового ящика:» введите admin, а в поля «Пароль» и «Подтверждение пароля» введите «P@ssw0rd» (без кавычек).
5. Убедитесь что параметр «Создать пользователя для этого почтового ящика» включен и нажмите «OK».

6. В появившемся окне будут отображены сведения для настройки почтового клиента на использование созданного ящика. Запомните или запишите их.
7. Аналогичным образом создайте почтовые ящики `user01` и `user02`. В качестве пароля используйте «P@ssw0rd».

5.8.3. Упражнение 3. Настройка почтового клиента на сервере serverOl

Вы настроите программу OutlookExpressна компьютере serverOlна использование почтового ящика `admin@test.local`

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. Запустите программу OutlookExpress. Для этого выполните «Пуск | Программы | OutlookExpress».
3. Выполните команду «Сервис | Учетные записи».
4. Нажмите кнопку «Добавить» и выберите пункт «Почта...».
5. На странице «Введите имя» в поле «Выводимое имя:» введите «Admin» и нажмите «Далее».
6. На странице «Адрес электронной почты Интернета» в поле «Электронная почта:» введите «admin@test.local» и нажмите «Далее».
7. На следующей странице в полях «Сервер входящих сообщений» и «Сервер исходящих сообщений» введите «serverOl» и нажмите «Далее».
8. На следующей странице в поле «Учетная запись:» введите «admin@test.local». В поле «Пароль:» введите «P@ssw0rd» и нажмите кнопку «Далее».
9. На последней странице нажмите кнопку «Готово».
10. Закройте окно «Учетные записи в Интернете».
11. На панели инструментов нажмите кнопку «Доставить почту». Если сообщений об ошибках не появляется и не запрашивается пароль, то почту Вы настроили верно. Проверьте папку «Входящие». Там не должно быть новых сообщений.
12. Создайте тестовое письмо на адрес user01@test.localи отправьте его.

5.8.4. Упражнение 4. Настройка почтовых клиентов на компьютере clientOl

Вы настроите программу OutlookExpressна компьютере client01 для доменной учетной записи user01 на использование почтового ящика `user01@test.local`и для доменной учетной записи user02 на использование почтового ящика `user02@test.local`.

1. Зарегистрируйтесь на компьютере client01 под доменной учетной записью user01 с паролем P@ssw0rd.
2. Запустите программу OutlookExpress. Для этого выполните «Пуск | Все программы | OutlookExpress».
3. Выполните команду «Сервис | Учетные записи».

4. Нажмите кнопку «Добавить» и выберите пункт «Почта...».
5. На странице «Введите имя» в поле «Выводимое имя:» введите «User01» и нажмите «Далее».
6. На странице «Адрес электронной почты Интернета» в поле «Электронная почта:» введите «user01@test.local» и нажмите «Далее».
7. На следующей странице в полях «Сервер входящих сообщений» и «Сервер исходящих сообщений» введите «server01» и нажмите «Далее».
8. На следующей странице в поле «Учетная запись:» введите «user01@test.local». В поле «Пароль:» введите «P@ssw0rd» и нажмите кнопку «Далее».
9. На последней странице нажмите кнопку «Готово».
10. Закройте окно «Учетные записи в Интернете».
11. На панели инструментов нажмите кнопку «Доставить почту». Если сообщений об ошибках не появляется и не запрашивается пароль, то почту Вы настроили верно. Проверьте папку «Входящие». Там должно быть одно новое тестовое письмо от адресата «Admin».
12. Создайте тестовое письмо на адрес user02@test.localи отправьте его.
13. Завершите сеанс пользователя user01 на компьютере client01.
14. Зарегистрируйтесь на компьютере client01 под доменной учетной записью user02 с паролем P@ssw0rd.
15. Выполните пункты 2-10 для настройки программы OutlookExpressна использование почтового ящика user02@test.local.
16. На панели инструментов нажмите кнопку «Доставить почту». Если сообщений об ошибках не появляется и не запрашивается пароль, то почту Вы настроили верно. Проверьте папку «Входящие». Там должно быть одно новое тестовое письмо от адресата «User01».
17. Завершите сеанс пользователя user02 на компьютере client01.

5.9. Лабораторная работа № 2. Развертывание антивирусной защиты

В этой лабораторной работе на компьютер server01 вы установите MSDE2000SP3, Kaspersky® AdministrationKit, Антивирус Касперского® для WindowsFileServers. На компьютер client01 вы удаленно установите Агент администрирования и Антивирус Касперского® для WindowsWorkstations.

Предварительные требования

Для выполнения данной работы необходимо наличие двух компьютеров (можно виртуальных) подготовленных в лабораторной работе №1. Необходимо наличие дистрибутивов MSDE2000 SP3 (поставляется в комплекте с Kaspersky® AdministrationKit), Kaspersky® AdministrationKit, Антивирус Касперского® для WindowsFileServers, Антивирус Касперского® для WindowsWorkstations. Необходимо наличие лицензионных клю

чей для продуктов Антивирус Касперского® для WindowsFileServersи Антивирус Касперского® для WindowsWorkstations.

На клиентском компьютере с ОС WindowsXPSP2 должно быть включено исключение «Общий доступ к файлам и принтерам» и открыт порт UDP15000.

Лабораторная работа №2 выполняется на компьютере server01. Компьютер client01 должен быть включен.

5.9.1. Упражнение 1. Установка MSDE2000

Вы установите на компьютер server01 MSDE2000 SP3.

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. Запустите на выполнение файл msde2ksp3ru.exe. Следуйте указаниям мастера установки. Все предлагаемые параметры нужно оставить без изменения. Если после установки потребуется перезагрузка - перезагрузите компьютер.

5.9.2. Упражнение 2. Установка Kaspersky® Administration Kit

Вы установите на компьютер server01 Сервер и консоль администрирования из комплекта Kaspersky® AdministrationKit.

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. Запустите на выполнение файл установки. В нашем случае это будет kasp5.0.1152_adminkitru.exe.
3. В окне приветствия Мастера установки нажмите кнопку «Далее».
4. В появившемся окне выберите путь для сохранения распакованного дистрибутива и нажмите «Далее».
5. После появления приветствия Мастера установки, нажмите кнопку «Далее».
6. Ознакомьтесь с лицензионным соглашением и если Вы его принимаете, нажмите кнопку «Да».
7. На следующей странице введите данные о пользователе и организации обладающей лицензией на использование программы. Нажмите кнопку «Далее».
8. На странице «Каталог установки» нажмите кнопку «Далее».
9. На странице выбора компонентов включите компонент «Сервер администрирования» (Консоль администрирования устанавливается автоматически). Нажмите кнопку «Далее».
10. На следующей странице выберите вариант «Учетная запись пользователя» и нажмите кнопку «Далее».
11. На следующей странице нажмите кнопку «Создать».

12. В появившемся окне укажите имя создаваемой учетной записи и пароль. Например, имя - KasperskyAdminKit, пароль - P@ssw0rd. Нажмите кнопку «Далее».
13. В появившемся окне нажмите кнопку «Далее».
14. При появлении информационного сообщения о том какие права будут дополнительно присвоены указанной Вами учетной записи, нажмите кнопку «OK».
15. На следующей странице проверьте, что в поле «Имя SQL-сервера:» выставлено значение «(local)», в поле «Имя базы данных SQL-сервера:» - «KAV» и нажмите кнопку «Далее».
16. На странице выбора режима SQL-аутентификации, выберите вариант «Режим аутентификации MicrosoftWindows» и нажмите кнопку «Далее».
17. На странице «Создание папки общего доступа», выберите вариант «Создать новую папку общего доступа». В поле «Имя папки общего доступа:» введите «AVPSHARE» и нажмите кнопку «Далее».
18. На следующей странице Вам будет предложено указать номера портов для подключения к Серверу администрирования. Если на компьютере, где установлен Сервер администрирования работает межсетевой экран (например, это компьютер под управлением ОС WindowsXPc ServicePack2 или WindowsServer2003 R2), то необходимо открыть указанные порты вручную для нормального функционирования Сервера администрирования. Нажмите кнопку «Далее».
19. На странице «Создание сертификата Сервера администрирования» выберите «Создать новый сертификат», выключите параметр «Сохранить резервную копию сертификата» и нажмите кнопку «Далее».
20. На странице «Просмотр параметров установки» нажмите кнопку «Далее».
21. После завершения установки, нажмите кнопку «Готово».

5.9.3. Упражнение 3. НастройкаKaspersky® Administration Kit.

Вы выполните первоначальную настройку Сервера администрирования.

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
3. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования». При первом подключении, Вы увидите предложение запустить Мастер первоначальной настройки. Нажмите кнопку «Запустить Мастер первоначальной настройки». Если же окно с предложением запустить Мастер первоначальной настройки

не появилось, вызовите контекстное меню для корневого узла «Сервер администрирования» и выполните команду «Мастер первоначальной настройки».

4. В окне приветствия Мастера первоначальной настройки нажмите кнопку «Далее».
5. Дождитесь завершения опроса сети. Щелкните по надписи «Просмотреть результаты опроса сети» и убедитесь, что в ходе опроса были обнаружены компьютеры serverOlи clientOl. Закройте окно с результатами опроса сети и на странице «Опрос сети» нажмите кнопку «Далее».
6. На странице «Логическая сеть» выберите вариант «Сформировать логическую сеть на основе Windows-сети» и нажмите «Далее».
7. На странице «Параметры уведомления» задайте адрес получателя - admin@test.local, адрес почтового сервера - serverOl, номер SMTP- порта - 25 и нажмите кнопку «Далее».
8. На странице «Система антивирусной защиты» нажмите кнопку «Параметры» чтобы задать параметры Задачи получения обновлений.
9. В окне «Параметры» выберите «Загружать только выбранные обновления». В качестве источника обновления задайте каталог обновлений «C:\update». Для этого нажмите кнопку «Добавить...».
10. В появившемся окне выберите источник обновления «Каталог обновлений» и задайте адрес «C:\update». Нажмите кнопку «ОК».
11. Вернувшись в окно «Параметры», удалите источник обновления «Сервис обновлений Лаборатории Касперского». Для этого выделите его и нажмите кнопку «Удалить». Нажмите кнопку «ОК». Вы вернетесь на страницу «Система антивирусной защиты» Мастера первоначальной настройки.
12. Нажмите кнопку «Далее». Дождитесь появления сообщения о завершении работы Мастера первоначальной настройки.
13. Отключите параметр «Запустить Мастер удаленной установки» и нажмите кнопку «Готово».
14. В Консоли администрирования KasperskyAdministrationKitразверните узел «Группы» и папку «TEST». Окно Консоли администрирования KasperskyAdministrationKitдолжно выглядеть примерно следующим образом (рис. 5.92):

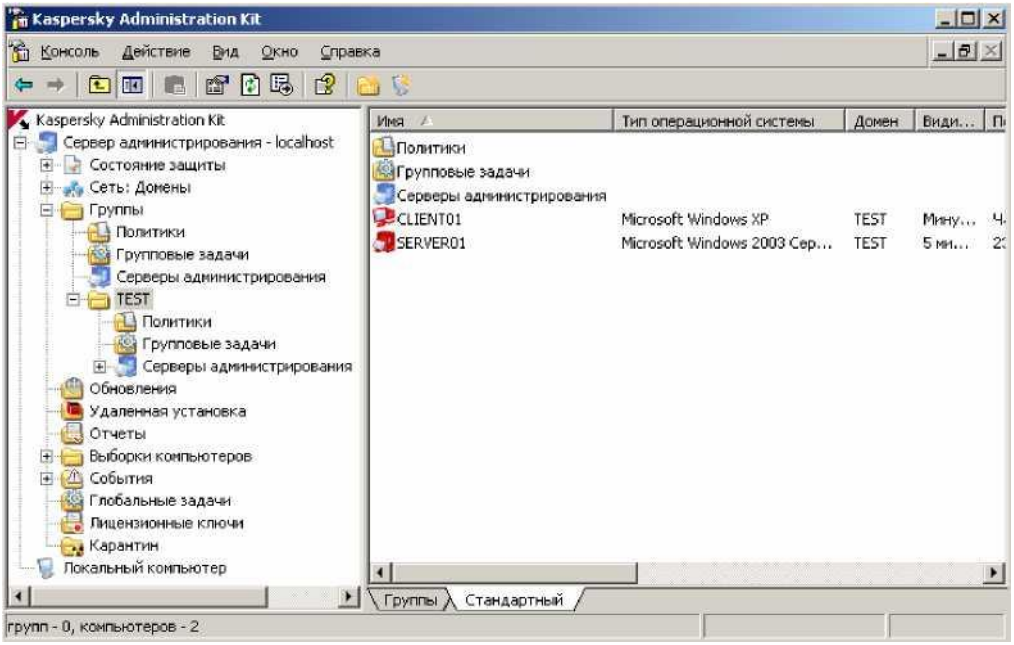

Рис. 5.92. Консоль администрирования

5.9.4. Упражнение 4. Удаленная установка Агента администрирования

Вы выполните форсированную установку Агента администрирования на клиентский компьютер clientOl.

1. Зарегистрируйтесь на компьютере serverOlпод доменной учетной записью Administrator с паролем P@ssw0rd.
2. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
3. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования».
4. В левой части Консоли администрирования выберите узел «Удаленная установка». В правой части окна вызовите контекстное меню элемента «Инсталляционный пакет Агент администрирования» и выполните команду «Установить».
5. После запуска Мастера создания задачи удаленной установки, нажмите кнопку «Далее».
6. На следующей странице задайте имя для Задачи удаленной установки (например, «Установка Инсталляционный пакет Агент администрирования») и нажмите кнопку «Далее».
7. На странице «Метод установки» выберите «Форсированная установка» и нажмите кнопку «Далее».
8. На странице «Настройки» включите параметр «Средствами Windowsиз папки общего доступа» и отключите параметр «С помощью Агента администрирования». Остальные параметры оставьте без изменения и нажмите кнопку «Далее».

9. На странице «Способ выбора клиентских компьютеров» выберите вариант «На основании данных, полученных в ходе опроса Windows-сети» и нажмите кнопку «Далее».
10. На следующей странице разверните раздел «Группы | TEST», отметьте компьютер «Client01» и нажмите кнопку «Далее».
11. На следующей странице выберите вариант «Учетная запись по умолчанию» и нажмите кнопку «Далее».
12. На странице «Расписание запуска задачи» выберите вариант «Немедленно» и нажмите кнопку «Далее».
13. На странице «Создание задачи» нажмите кнопку «Далее».
14. При появлении сообщения об успешности создания задачи «Установка Инсталляционный пакет Агент администрирования», завершите работу Мастера, нажав кнопку «Готово».
15. В левой части Консоли администрирования выберите «Глобальные задачи». В правой части окна Вы увидите созданную задачу «Установка Инсталляционный пакет Агент администрирования». Дождитесь завершения этой задачи (значок этой задачи изменится с ^ на У). Вызовите контекстное меню этой задачи (см. рис. 5.46) и выполните команду «Результаты».
16. Удостоверьтесь, что задача была успешно завершена на компьютере client01 (в правой части окна будет присутствовать сообщение «Удаленная установка на клиентском компьютере успешно завершена»). Нажмите кнопку «Закрыть».
17. С помощью контекстного меню этой задачи вызовите окно свойств. Оно должно выглядеть примерно следующим образом (рис. 5.93):

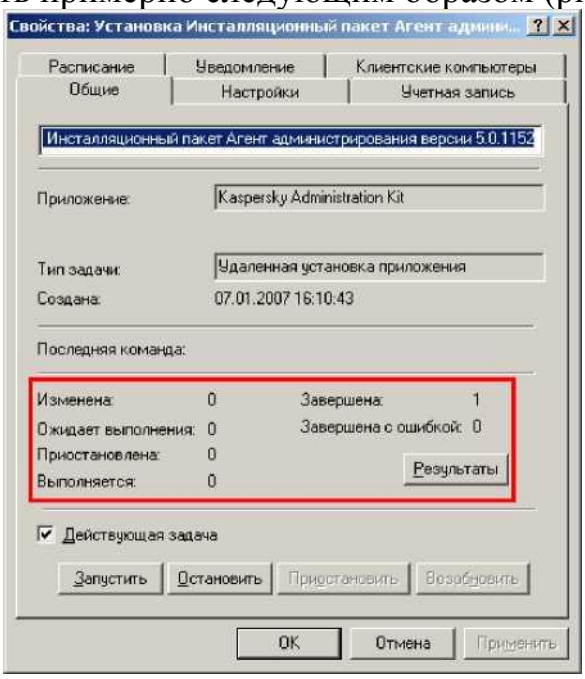

Рис. 5.93. Окно свойств задачи

5.9.5. Упражнение 5. Удаленная установка Антивируса Касперского® для WindowsWorkstations

Вы создадите Инсталляционный пакет Антивируса Касперского 5.0 для WindowsWorkstation, а также задачу удаленной установки этого пакета на клиентский компьютер client01.

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. Для создания Инсталляционного пакета Антивируса Касперского 5.0 для WindowsWorkstationвам понадобится распакованный дистрибутив этого продукта. Если у вас есть только упакованный дистрибутив (в виде единственного исполнимого файла), то для его распаковки выполните пункты 3-7. Иначе перейдите к пункту 8.
3. Запустите на выполнение файл установки Антивируса Касперского 5.0 для WindowsWorkstation. В нашем случае это будет kav5.0.712_winwksru.exe.
4. В окне приветствия программы «InstallShieldWizard» нажмите кнопку «Далее».
5. В окне «Папка для сохранения файлов» укажите путь для сохранения распакованного дистрибутива (C:\KAV\WinWorkstation\Russian) и нажмите «Далее».
6. При появлении окна «Добро пожаловать в Мастер установки Антивируса Касперского для WindowsWorkstation» нажмите кнопку «Отмена». На вопрос «Вы действительно хотите прервать установку Антивируса Касперского для WindowsWorkstation» нажмите кнопку «Да».
7. В окне «Установка прервана» нажмите «OK». Теперь в папке «C:\KAV\WinWorkstation\Russian» находится распакованный дистрибутив Антивируса Касперского 5.0 для WindowsWorkstation.
8. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
9. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования».
10. В левой части Консоли администрирования вызовите контекстное меню узла «Удаленная установка» и выполните команду «Создать | Инсталляционный пакет».
11. После запуска Мастера создания инсталляционного пакета, нажмите кнопку «Далее».
12. На странице «Имя инсталляционного пакета» введите имя (например, «Инсталляционный пакет Антивирус Касперского для WindowsWorkstation») и нажмите кнопку «Далее».
13. На странице «Приложение» выберите «Создать инсталляционный пакет для приложения Лаборатории Касперского». С помощью кнопки «Обзор» укажите расположение файла workstations.kpdиз распакованного

дистрибутива Антивируса Касперского для WindowsWorkstation. После указания файла, нажмите кнопку «Далее».

14. На странице «Выбор лицензии» с помощью кнопки «Обзор...» укажите файл с лицензионным ключом и нажмите кнопку «Далее».
15. На странице «Загрузка инсталляционного пакета» нажмите кнопку «Далее».
16. Если во время загрузки инсталляционного пакета появится предупреждение, показанное на рис. 5.94, нажмите кнопку «Открыть» и загрузка будет продолжена.

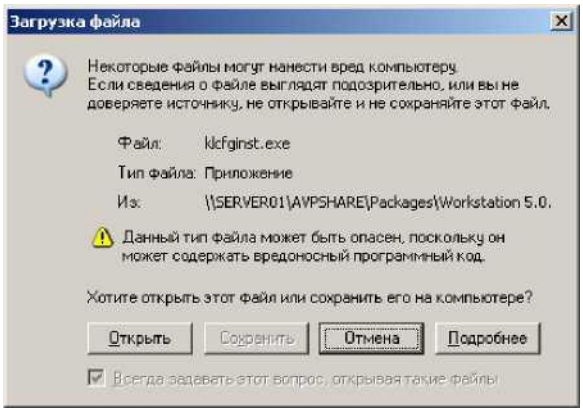

Рис. 5.94. Предупреждение ОС

17. На странице «Завершение работы Мастера.» нажмите кнопку «Готово».
18. С помощью контекстного меню инсталляционного пакета, выполните команду «Свойства». Ознакомьтесь с содержимым всех закладок в окне свойств Инсталляционного пакета.
19. Закройте окно свойств Инсталляционного пакета.
20. Аналогично упражнению № 4 в этой Лабораторной работе, создайте задачу удаленной установки на основе созданного нами инсталляционного пакета и выполните её.
21. Проверьте результаты выполнения созданной задачи. На рис. 5.95 представлен возможный результат.

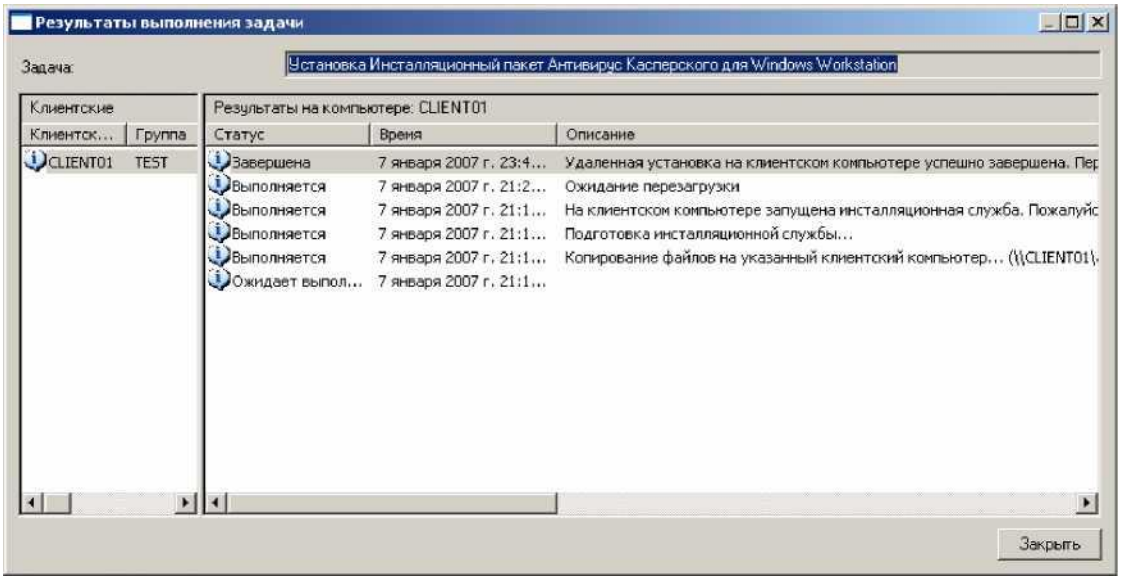

Рис. 5.95. Результаты успешного выполнения задачи

5.9.6. Упражнение 6. Удаленная установка Антивируса Касперского® для WindowsFileServers

Вы создадите Инсталляционный пакет **Антивируса Касперского 5.0 для WindowsFileServers**, а также задачу удаленной установки этого пакета на компьютер **server01**.

Упражнение выполняется аналогично упражнению 5.

Не забудьте проверить успешность выполнения этой задачи. На рис. 5.96 представлен возможный результат.

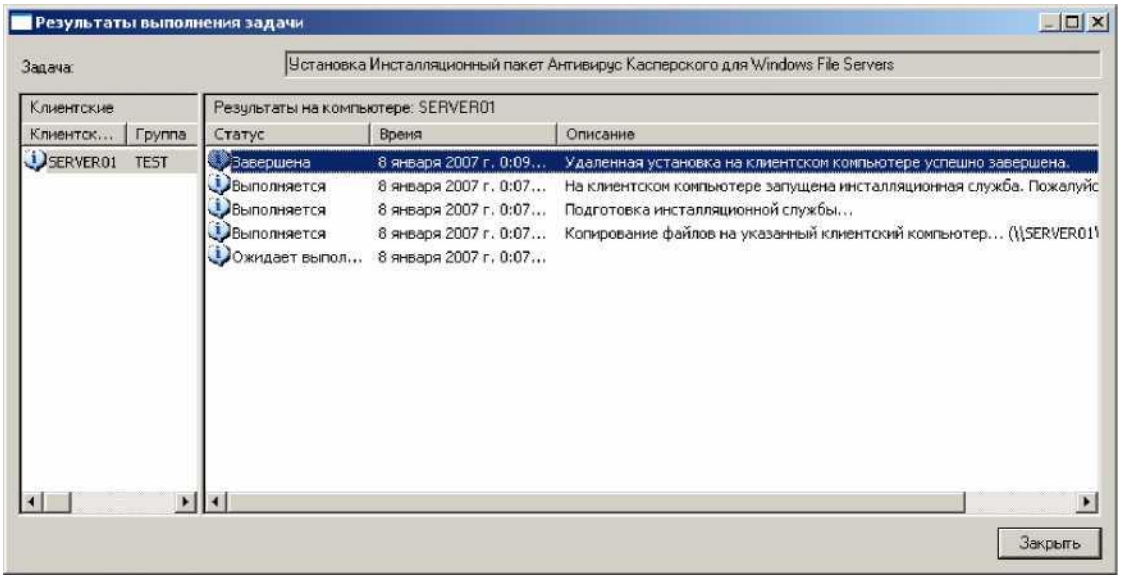

Рис. 5.96. Результаты выполнения задачи

5.10. Лабораторная работа № 3. Примеры практического использования

В этой лабораторной работе Вы разберете примеры практического использования Антивирусных продуктов Лаборатории Касперского под управлением Сервера администрирования. Вы обновите антивирусные базы на Сервере администрирования и распространите их на компьютеры server01 и client01. Настроите параметры уведомления о событиях, ознакомитесь с реакцией на обнаружение тестового «вируса» на диске и в почтовом сообщении. Просмотрите отчеты по различным критериям. Настроите задачу резервного копирования данных сервера администрирования и выполните восстановление данных Сервера администрирования из резервной копии.

Предварительные требования

Для выполнения данной работы необходимо наличие двух компьютеров (можно виртуальных) подготовленных в лабораторных работах №1 и №2. Необходимо наличие тестового «вируса» Eicarи свежих антивирусных баз.

Загрузить тестовый "вирус" можно с официального сайта организации EICAR: http://www.eicar.org/anti virus test file.htm[8].

Лабораторная работа №3 выполняется на компьютерах server01 и client01.

5.10.1. Упражнение 1. Обновление антивирусных баз (+ автоматическое распространение обновлений).

Вы настроите задачу получения обновлений Сервером администрирования и настроите задачи получения обновлений Антивирусами на компьютерах server01, client01.

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
3. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования».
4. Проверьте дату создания антивирусных баз на компьютере server01. Для этого разверните узел «Группы» и папку «TEST». В правой части Консоли администрирования вызовите контекстное меню для компьютера Server01. Выполните команду «Приложения». Откроется закладка «Приложения» в окне свойств компьютера server01. Выберите приложение «Антивирус Касперского ...» и нажмите кнопку «Свойства». В появившемся окне «Параметры приложения.» на закладке «Общие» просмотрите дату создания «Антивирусных баз».

5. Аналогичным образом проверьте дату создания антивирусных баз на компьютере clientOl.
6. Откройте папку «Групповые задачи» узла «Группы». Запомните названия существующих там задач. Проверьте что задач с названием «Автоматическое обновление - Антивирусные базы» там нет.
7. Включите механизм «Автоматического распространения обновлений». Для этого откройте свойства узла «Обновления» и включить параметр «Автоматически распространять обновления антивирусных баз на клиентские компьютеры». Нажмите кнопку «ОК».
8. Откройте папку «Групповые задачи» узла «Группы». Проверьте что там появились две задачи «Автоматическое обновление - Антивирусные базы». Одна для Антивируса Касперского для WindowsWorkstation, другая для Антивируса Касперского для WindowsFileServers. При получении обновлений Сервер администрирования будет запускать эти задачи автоматически [7].
9. Откройте свойства задачи «Автоматическое обновление - Антивирусные базы» приложения «Антивирус Касперского для WindowsWorkstation». Перейдите на закладку «Расписание». Проверьте что параметр «Запуск по расписанию» выставлен в положение «Вручную». Выключите параметр «Распределить запуск задачи случайным образом в интервале (мин.):». Нажмите кнопку «ОК».
10. Аналогичным образом проверьте расписание задачи «Автоматическое обновление - Антивирусные базы» приложения «Антивирус Касперского для WindowsFileServers».
11. Скопируйте в папку «C:\update» свежие антивирусные базы.
12. В левой части Консоли администрирования выберите узел «Глобальные задачи». С помощью контекстного меню откройте свойства задачи «Задача получения обновлений Сервером администрирования».
13. В окне свойств, перейдите на закладку «Настройки». Проверьте что в качестве источника обновлений указана папка «C:\update». Перейдите на закладку «Общие» и нажмите кнопку «Запустить».
14. Дождитесь завершения задачи. Нажмите кнопку «Результаты». Проверьте, что задача успешно завершена.
15. Убедитесь что новые антивирусные базы автоматически распространены на компьютеры server01 и client01. Для этого повторите действия пунктов 4,5.
16. Если дата создания антивирусных баз осталось прежней, то выполните синхронизацию данных компьютеров server01 и client01 с данными Сервера администрирования. Для этого разверните узел «Группы» и папку «TEST». В правой части Консоли администрирования вызовите контекстное меню для компьютера Server01. Выполните команду «Синхронизировать». Выполните аналогичное действие с компьютером client01.

17. Ещё раз проверьте дату создания антивирусных баз на компьютерах serverOlи clientOl(Для этого повторите действия пунктов 4,5). Теперь дата должна измениться.

5.10.2. Упражнение 2. Настройка параметров уведомлений о событиях

Вы зададите адрес электронного почтового ящика администратора и определите события на компьютере clientOlдля уведомления администратора по электронной почте.

1. Зарегистрируйтесь на компьютере serverOlпод доменной учетной записью Administrator с паролем P@ssw0rd.
2. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
3. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования».
4. Откройте окно свойств Сервера администрирования.
5. Перейдите на закладку «Уведомления». Проверьте, что адрес получателя - admin@test.local,адрес SMTP-сервера - serverOl, номер порта SMTP-сервера - 25. Нажмите кнопку «ОК».
6. Откройте узел «Группы». В папке «Политики» откройте свойства «Политики Антивируса Касперского для WindowsWorkstations».
7. Перейдите на закладку «События».
8. Выберите уровень важности «Критическое событие». Выберите тип события - «Найден вирус». Включите параметр «Уведомлять по электронной почте».
9. Выберите уровень важности «Предупреждение». Включите параметр «Уведомлять по электронной почте» для событий «Объект вылечен», «Зараженный объект удален», «Объект не вылечен». Нажмите кнопку «Применить».
10. Перейдите на закладку «Применение» и нажмите кнопку «Изменить сейчас». Нажмите кнопку «Подробно» и убедитесь что политика применена для компьютера clientOl.

5.10.3. Упражнение 3. Обнаружение тестового «вируса» на диске.

Вы ознакомитесь с реакцией Антивируса Касперского для Windows Workstations на файловый вирус.

1. Зарегистрируйтесь на компьютере serverOlпод доменной учетной записью Administrator с паролем P@sswOrd.
2. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
3. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования».

4. Остановите постоянную защиту файлов на компьютере serverOl. Для этого разверните узел «Группы» и папку «TEST». В правой части Консоли администрирования вызовите контекстное меню для компьютера ServerOl. Выполните команду «Задачи». Откроется закладка «Задачи» в окне свойств компьютера serverOl. Выберите задачу «Постоянная защита файлов» и нажмите кнопку «Свойства». В появившемся окне «Свойства задачи...» на закладке «Общие» нажмите кнопку «Остановить». Нажмите кнопку «OK». Нажмите кнопку «OK».
5. Скопируйте файл eicar.comв папку \\server01\AVPSHARE.
6. Переключитесь на компьютер client01.
7. Зарегистрируйтесь на компьютере client01 под доменной учетной записью User01 с паролем P@ssw0rd.
8. Скопируйте файл \\server01\AVPSHARE\eicar.comна рабочий стол. Для этого выполните «Пуск | Выполнить». Наберите «\\server01\AVPSHARE». Нажмитекнопку«OK». Перетащите левой кнопкой мыши файл eicar.comна рабочий стол.
9. На экране появится сообщение (см. рис. 5.97). Антивирус не дает возможности обратиться к файлу с вирусом.

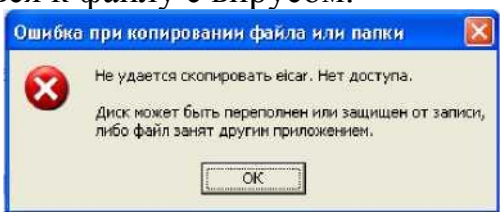

Рис. 5.97. Сообщение ОС

10. Переключитесь на компьютер server01.
11. Разверните узел «События» и папку «Все события». В правой части Консоли администрирования вы увидите события с уровнем важности «Критическое». Откройте свойства последнего события. В поле «Описание» вы увидите «Объект \\server01\AVPSHARE\eicar.comзаражен вирусом EICAR-Test-File(Пользователь: user01)». Закройте окно с описанием события.
12. Разверните узел «Группы» и папку «TEST». В правой части Консоли администрирования вызовите контекстное меню для компьютера client01. Выполните команду «События». В появившемся окне просмотрите свойства обнаруженных событий. Описание последнего события будет: «Объект \\server01\AVPSHARE\eicar.comзаражен вирусом EICAR-Test-File (Пользователь: user01)». Закройте окно «Параметры события». Закройте окно «События».
13. Откройте окно свойств компьютера client01. Для этого дважды щелкните по значку CLIENT01 в папке «TEST» узла «Группы». На закладке «Защита» вы увидите количество обнаруженных вирусов. Нажмите кнопку «OK».

14. Запустите программу OutlookExpress. Откройте папку «Входящие». Вы увидите сообщения от «KasperskyAdministrationServer» (см. рис. 5.98)

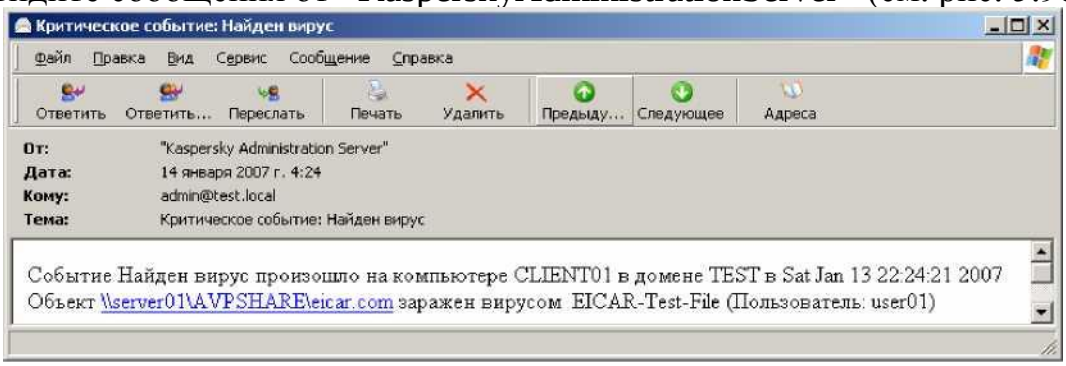

Рис. 5.98. Уведомление о событии

5.10.4. Упражнение 4. Обнаружение тестового «вируса» в почтовом сообщении

Вы познакомитесь с реакцией Антивируса Касперского для Windows Workstationsна вирус в почтовом сообщении.

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. Запустите программу OutlookExpress. Создайте письмо для адресата user01@test.localс темой «Новый файл» и текстом «Привет! Высылаю новый файл!». Прикрепите к письму файл \\server01\AVPSHARE\eicar.comи отправьте его.
3. Переключитесь на компьютер client01.
4. Зарегистрируйтесь на компьютере client01 под доменной учетной записью User01 с паролем P@ssw0rd.
5. Запустите программу OutlookExpress. Откройте папку «Входящие». Вы увидите уже обезвреженное сообщение от пользователя Admin(см. рис. 5.99) без вложенного файла.

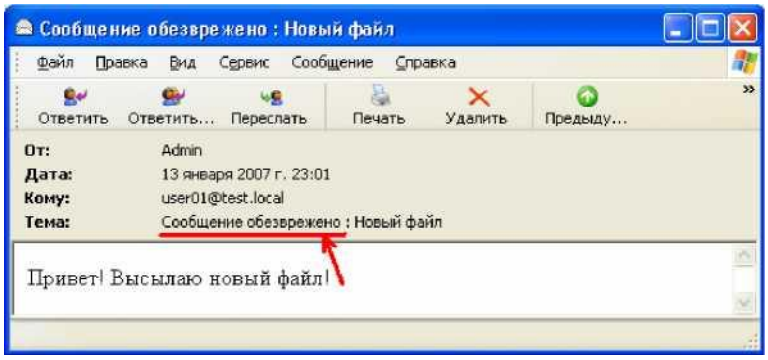

Рис. 5.99. Обезвреженное письмо

6. Переключитесь на компьютер server01.
7. Разверните узел «События» и папку «Все события». В правой части Консоли администрирования вы увидите одно событие с уровнем важ-

ности «Критическое» и два с уровнем «Предупреждение». Откройте свойства этих событий и ознакомьтесь с их описаниями.

8. Разверните узел «Группы» и папку «TEST». В правой части Консоли администрирования вызовите контекстное меню для компьютера clientOl. Выполните команду «События». В появившемся окне просмотрите свойства последних обнаруженных событий (одно событие с уровнем важности «Критическое» и два с уровнем «Предупреждение»).
9. Откройте окно свойств компьютера clientOl. Для этого дважды щелкните по значку CLIENT01 в папке «TEST» узла «Группы». На закладке «Защита» вы увидите что количество обнаруженных вирусов увеличилось.
10. Запустите программу OutlookExpress. Откройте папку «Входящие». Вы увидите два новых письма от «KasperskyAdministrationServer» («Критическое событие: Найден вирус», «Предупреждение: Зараженный объект удален»).
11. Запустите постоянную защиту файлов на компьютере server01. Для этого разверните узел «Группы» и папку «TEST». В правой части Консоли администрирования вызовите контекстное меню для компьютера Server01. Выполните команду «Задачи». Откроется закладка «Задачи» в окне свойств компьютера server01. Выберите задачу «Постоянная защита файлов» и нажмите кнопку «Свойства». В появившемся окне «Свойства задачи...» на закладке «Общие» нажмите кнопку «Запустить». Нажмите кнопку «ОК». Нажмите кнопку «ОК».

5.10.5. Упражнение 5. Просмотр отчетов

Вы познакомитесь с существующими шаблонами отчетов и настроите автоматическую ежедневную рассылку отчета о версиях антивирусных баз.

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
3. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования».
4. Откройте узел «Отчеты».
5. Выберите Отчет о версиях антивирусных баз. Двойным щелчком по отчету откройте окно свойств.
6. На закладке «Общие» нажмите кнопку «Создать отчет».
7. В открывшемся окне Обозревателя InternetExplorerпросмотрите отчет.
8. Создайте и просмотрите отчеты с помощью остальных шаблонов.
9. Откройте контекстное меню «Отчет о версиях антивирусных баз». Выполните команду «Рассылка отчетов».

10. В окне приветствия Мастера создания рассылки отчета нажмите кнопку «Далее».
11. В окне «Имя задачи рассылки отчета» введите имя «Рассылка отчета о версиях антивирусных баз» и нажмите «Далее».
12. На странице «Параметры» выберите «Отчет о версиях антивирусных баз», введите адрес admin@test.local,тему «Антивирусные базы», выберите формат «Вложенный архив» и нажмите «Далее».
13. На странице «Учетная запись» выберите «Учетная запись по умолчанию» и нажмите «Далее».
14. На странице «Расписание запуска задачи» выберите «Ежедневно», «Каждый 2 день. Время запуска установите на 3 минуты позже текущего времени и нажмите «Далее».
15. На странице «Создание задачи» нажмите «Далее». На последней странице нажмите «Готово».
16. Запустите программу OutlookExpress. Выполните команду меню «Сервис | Параметры». На закладке «Безопасность» выключите параметр «Не разрешать сохранение или открытие вложении, которые могут содержать вирусы».
17. Откройте папку «Входящие». Вы увидите новое письмо от «KasperskyAdministrationServer» с темой «Антивирусные базы». Во вложенном файле в архиве .cabнаходится html-отчет и графические файлы. Распакуйте их в отдельную папку и откройте html-файл.

5.10.6. Упражнение 6. Резервное копирование данных сервера администрирования.

Вы настроите глобальную задачу резервного копирования данных Сервера администрирования, выполните её и с помощью созданной резервной копии восстановите данные Сервера администрирования.

1. Зарегистрируйтесь на компьютере server01 под доменной учетной записью Administrator с паролем P@ssw0rd.
2. На диске C: создайте папку «AVP_backup».
3. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
4. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования».
5. Откройте узел «Глобальные задачи».
6. Выберите задачу «Резервное копирование данных Сервера администрирования». Двойным щелчком по отчету откройте окно свойств этой задачи.
7. Откройте закладку «Параметры». В поле «Папка результата» задайте путь «C:\AVP_backup». В поля «Пароль для шифрования сертификата сервера», «Подтверждение пароля» введите P@ssw0rd.

8. Откройте закладку «Расписание». Задайте следующее расписание: Ежемесячно, каждый 1-ый день месяца, 22:00. Включите параметр «Запускать пропущенные задачи»
9. Откройте закладку «Уведомление». Параметр «Уведомлять о результатах» установите в значение «О любом результате» и включите параметр «Уведомлением по электронной почте».
10. Нажмите кнопку «Применить».
11. Откройте закладку «Общие» и нажмите кнопку «Запустить».
12. На время выполнения задачи соединение с Сервером администрирования будет разорвано, поэтому закройте окно свойств задачи и окно Консоли администрирования.
13. Запустите программу OutlookExpress. Откройте папку «Входящие».
14. Нажмите Ctrl+Мили выполните команду меню «Сервис | Доставить почту | Получить все».
15. Повторяйте пункт 15 до тех пор пока вы не получите новое письмо от «KasperskyAdministrationServer». В случае успешного завершения этой задачи, тема полученного сообщения будет «Задача "Резервное копирование данных Сервера администрирования" успешно завершена».
16. С помощью проводника откройте папку C:\AVP_backup. В ней должна появиться папка с названием «klbackupYYYY-MM-DD#HH-MM-SS». Запишите это название. В этой папке находится резервная копия.
17. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
18. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования».
19. Откройте узел «Глобальные задачи».
20. Удалите несколько глобальных задач.
21. Закройте окно Консоли администрирования KasperskyAdministrationKit.
22. Откройте окно командной строки. Для восстановления данных Сервера администрирования, выполните следующие команды:

cd "c:\ProgramFiles\KasperskyLab\KasperskyAdministrationKit"

klbackup.exe -logfile **restore1.log** -path "**C:\AVP_backup\klbackupYYYY-MM-DD#HH-MM-SS**" -restore -savecert **P@ssw0rd**

где **restore1.log**- имя файла для сохранения отчета,

"**C:\AVP_backup\klbackupYYYY-MM-DD#HH-MM-SS**" - имя папки с созданной резервной копией (см. пункт 16),

P@ssw0rd- пароль указанный при создании резервной копии (см. пункт 7)

23. Спомощьюблокнотапросмотритефайл"c:\Program Files\Kaspersky Lab\Kaspersky Administration Kit\restore1.log"

24. В случае успешности выполнения задачи восстановления в отчете последние три строчки будут такими:

    Operation completed successfully !

    Starting service CSAdminServer...OK
    Starting service KLNagent...OK
25. ЗапуститепрограммуKaspersky Administration Kit. Дляэтоговыполните «Пуск | Программы | Kaspersky Administration Kit | Kaspersky Administration Kit».
26. Подключитесь к Серверу администрирования, нажав на значок ± рядом с надписью «Сервер администрирования».
27. Откройте узел «Глобальные задачи».
28. Убедитесь, что глобальные задачи, которые были удалены в пункте 20, восстановлены.

5.11. Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал.

1. Перечислите возможные источники распространения угроз информационной безопасности.

2. Kaspersky® AdministrationKitпредназначен для удаленного централизованного управления всеми приложениями, входящими в состав продуктов Лаборатории Касперского, работающими на компьютерах под управлением операционных систем (выберите все варианты):
   a) Microsoft Windows;
   b) Linux;
   c) OS/2;
   d) Unix.

3. Возможность проверки почтового трафика по протоколам SMTP/POP3 вне зависимости от используемого почтового клиента отсутствует в следующих программных продуктах (выберите все варианты):
   a) Антивирус Касперского® для WindowsWorkstations;
   b) Антивирус Касперского® для WindowsFileServers;
   c) Kaspersky® Administration Kit.

4. Возможность лечения файлов в архивах ZIP, ARJ, CAB, RARотсутствует в следующих программных продуктах (выберите все варианты):
   a) Антивирус Касперского® для WindowsWorkstations;
   b) Антивирус Касперского® для WindowsFileServers;

c) Kaspersky® AdministrationKit.

5. Приложение KasperskyAdministrationKitсостоит из следующих компонентов (выберите все варианты):
   a) Сервер администрирования;
   b) Почтовый сервер;
   c) Почтовый клиент;
   d) Консоль администрирования;
   e) Агент администрирования.

6. Для удаленного управления Антивирусом Касперского® для WindowsFileServersc помощью Kaspersky® AdministrationKitнеобходимо на компьютер с установленным Антивирусом дополнительно установить (выберите все варианты):
   a) Сервер администрирования;
   b) Почтовый сервер;
   c) Почтовый клиент;
   d) Консоль администрирования;
   e) Агент администрирования.

7. При использовании в организации Сервера администрирования Kaspersky® AdministrationKitустановка антивирусных приложений на клиентские компьютеры возможна следующими методами (выберите все варианты):
   a) Локальная установка;
   b) Удаленная форсированная установка;
   c) Удаленная установка с помощью сценария запуска;
   d) Кроме локальной установки других вариантов не существует;
   e) Кроме удаленной установки других вариантов не существует.

8. Как функционирует форсированная удаленная установка приложений с помощью Сервера администрирования Kaspersky® Administration Kit?

9. По умолчанию, для доступа Сервера администрирования к компьютеру на котором установлен Агент администрирования используется следующий порт:
   a) UDP 139;
   b) TCP 139;
   c) UDP 445;
   d) TCP 445;
   e) UDP 15000;
   f) TCP 15000.

10. При использовании в организации Сервера администрирования Kaspersky® AdministrationKit, уведомление о событиях возможно следующими способами (выберите все варианты):

a) Уведомлением по электронной почте;

b) Уведомлением по сети средствами NETSEND;

c) Запуском исполняемого файла на компьютере под управлением Сервера администрирования;

d) Запуском исполняемого файла на клиентском компьютере.

e) Звуковым сигналом на компьютере под управлением Сервера администрирования.

5.12. Резюме

Современная антивирусная защита в организации с большим числом компьютеров невозможна без централизованного управления. Лаборатория Касперского для централизованной установки и управления своими антивирусными решениями на основе ОС MicrosoftWindowsпредлагает продукт KasperskyAdministrationKit. Возможности этого продукта гораздо шире чем описано в этом занятии. Подробное их описание можно найти в соответствующей документации.

В теоретической и лабораторной частях были рассмотрены основные действия необходимые для развертывания антивирусной защиты в организации с использованием KasperskyAdministrationKit, Антивируса Касперского® для WindowsFileServersи Антивируса Касперского® для WindowsWorkstations.

5.13. Литература

1. ***Прохоров А.*** Вредоносные программы, и как их победить // КомпьютерПресс.- 2006 .- №3.- С. 26-32.

2. Антивирус Касперского 6.0. Руководство пользователя // Лаборатория Касперского.- апрель 2006.- 214 с.

3. Описания вредоносных программ //Лаборатория Касперского, 2006. (http://www.viruslist.com/ru/viruses/encydopedia?chapter=152526512)

4. Kaspersky® CorporateSuite. Описание продукта // Лаборатория Касперского.- декабрь 2004.- 37 с.

5. Антивирус Касперского® 5.0 для WindowsWorkstations. Руководство администратора // Лаборатория Касперского.- декабрь 2004.- 166 с.

6. Антивирус Касперского® 5.0 для WindowsFileServers. Руководство администратора // Лаборатория Касперского.- декабрь 2004.- 111 с.

7. Kaspersky® AdministrationKit5.0. Руководство администратора // Лаборатория Касперского.- декабрь 2004.- 210 с.

8. Kaspersky® AdministrationKit5.0. Начало работы // Лаборатория Касперского.- декабрь 2004.- 26 с.

9. Обновления антивирусных баз // Лаборатория Касперского.- 2007. (http://www.kaspersky.ru/avupdates)