Тема: 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 BusinessOptimaIи 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, входящими в состав продуктов Лаборатории Касперского, работающими на

компьютерах под управлением операционной системы Windows. В том числе:

- объединение компьютеров в группы администрирования в соответст вии 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 от дельных компьютеров при помощи настроек приложения;
- централизованное управление работой приложений путем создания и запуска групповых и глобальных задач;
- построение индивидуальных схем работы приложений путем созда ния и запуска задач для набора компьютеров из различных групп ад- министрирования.

- 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 ин- терфейс 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 администри рования	• MSDE2000 с установленным Ser- vicePack3 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.

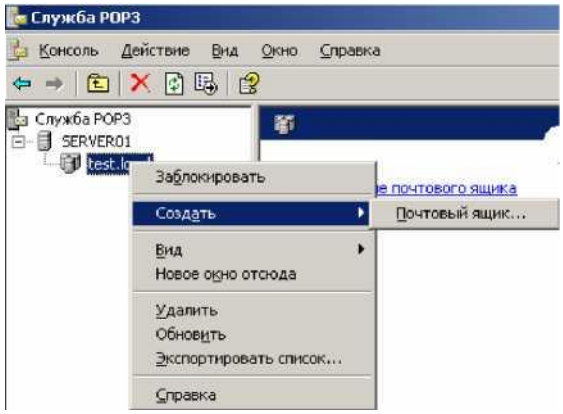


Рис. 5.1. Контекстное меню почтового сервера

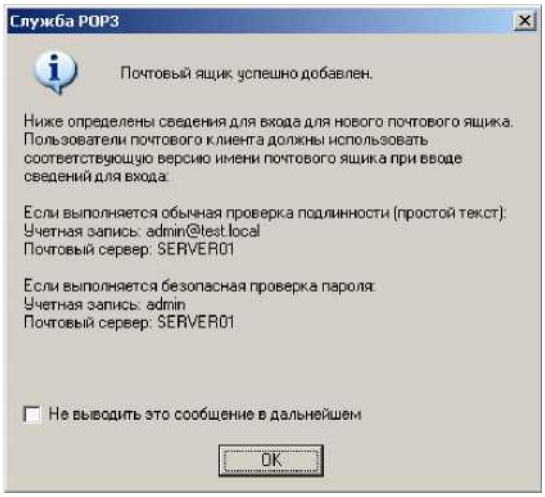


Рис. 5.2. Параметры для настройки почтового клиента

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 Out-lookExpress. 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. ВкомплектеKaspersky® 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).

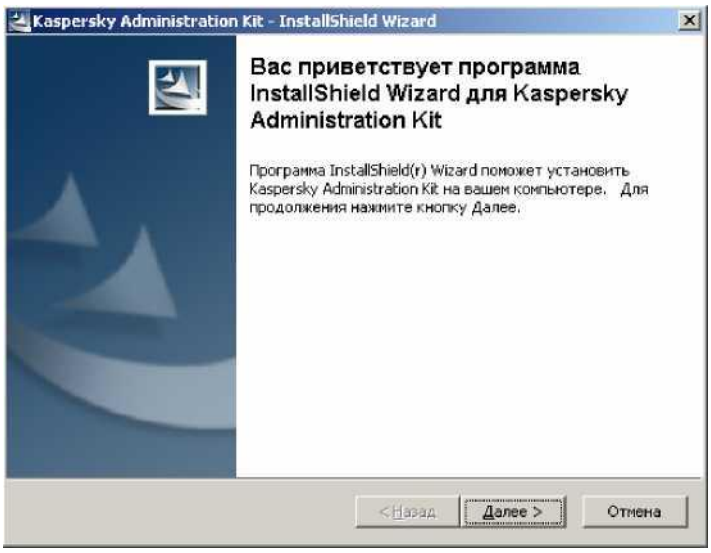


Рис. 5.3. Приветствие программы InstallShieldWizardНажмите кнопку «Далее». В появившемся окне выберите путь для сохранения распакованного дистрибутива (рис. 5.4). Нажмите «Далее».

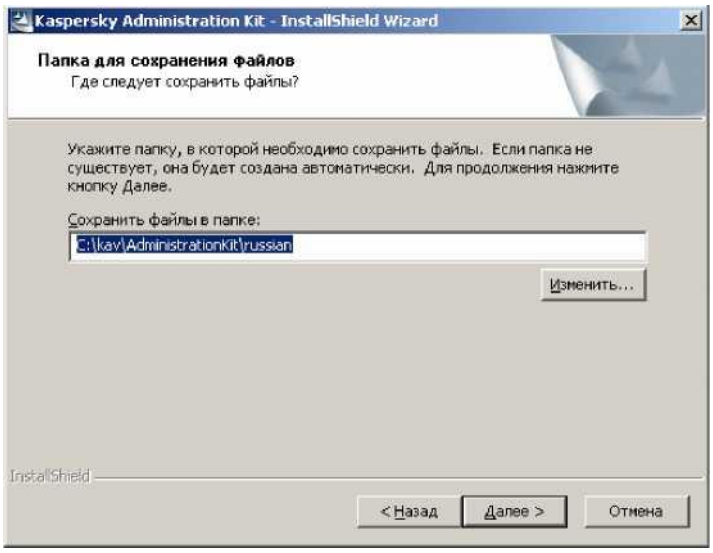


Рис. 5.4. Выбор папки для сохранения файлов После распаковки дистрибутива, на экране появится приветствие Мастера установки (рис. 5.5). Нажмите кнопку «Далее». Ознакомьтесь с лицензионным соглашением и если Вы его принимаете, нажмите кнопку «Да». На следующей странице введите данные о пользователе и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

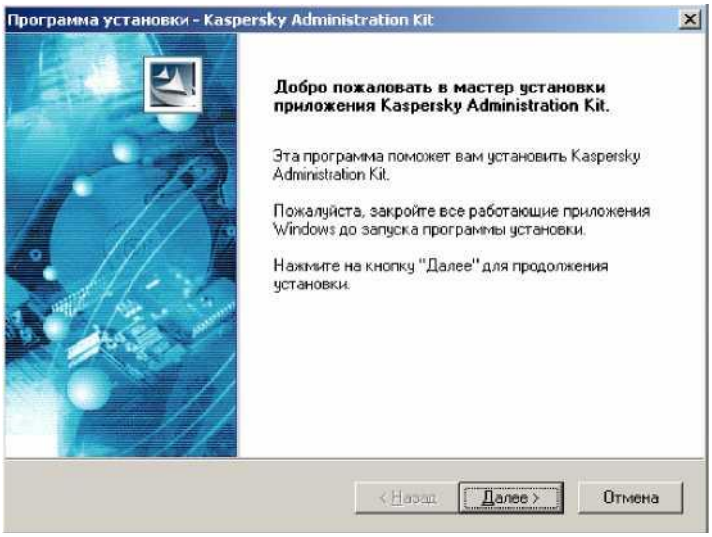


Рис. 5.5. Приветствие мастера установки KasperskyAdministrationKitНа следующей странице укажите каталог для установки программы (рис. 5.6). По умолчанию, программа будет устанавливаться в папку «%ProgramFiles%\KasperskyLab\KasperskyAdministrationKit\». Нажмите кнопку «Далее».

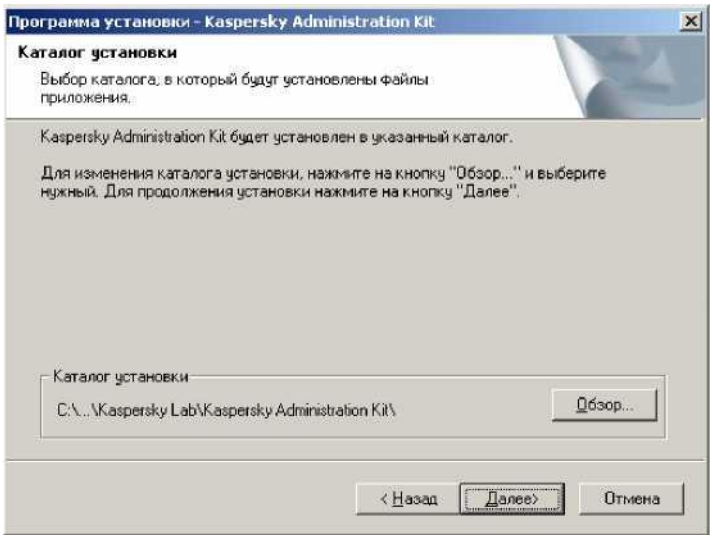


Рис. 5.6. Выбор каталога установки

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».

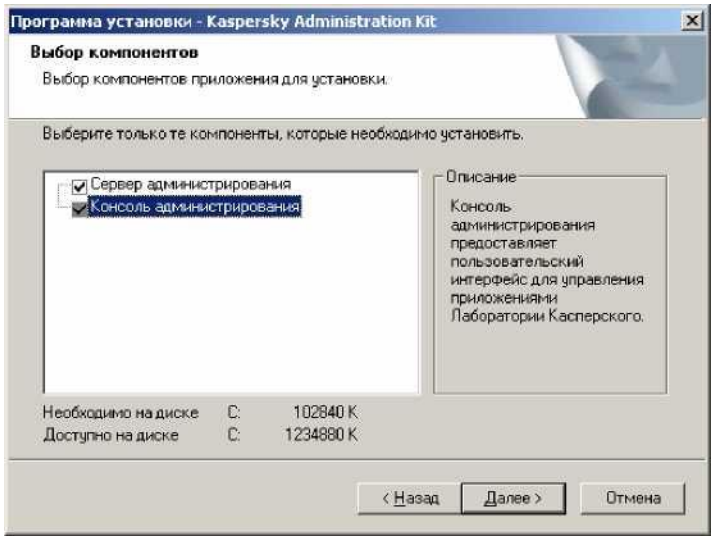


Рис. 5.7. Выбор компонентов для установки Так как мы выбрали установку Сервера администрирования, на следующей странице нам предлагается выбрать учетную запись для запуска службы Сервера администрирования (рис. 5.8). Только при использовании учетной записи пользователя с правами администратора домена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

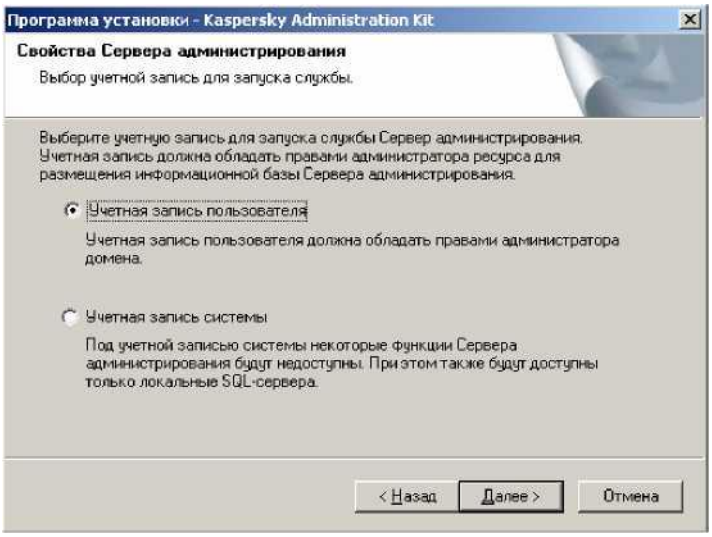


Рис. 5.8. Выбор учетной записи для запуска службы Сервера администрирования

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).

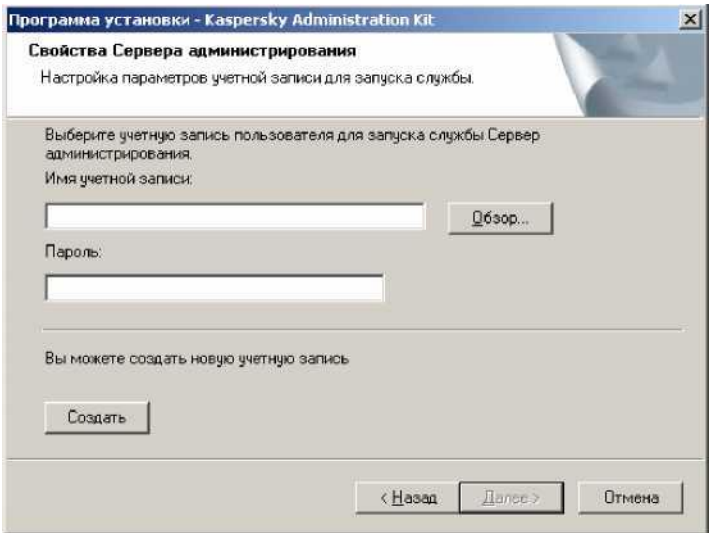


Рис. 5.9. Свойства сервера администрирования Нажмите кнопку «Создать». В появившемся окне укажите имя создаваемой учетной записи и пароль (рис. 5.10). Например, имя - KaspAdminKit, пароль - P@ssw0rd. Нажмите кнопку «Далее».

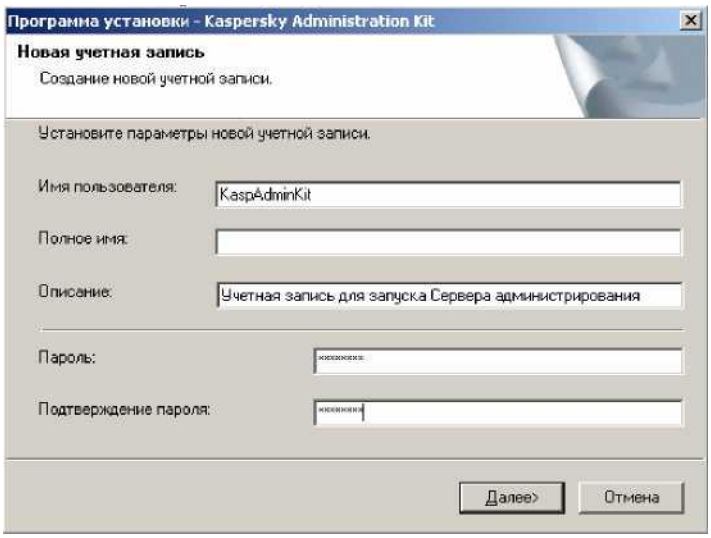


Рис. 5.10. Создание новой учетной записи Вы вернетесь к предыдущему окну, где уже будет указана созданная учетная запись (рис. 5.11). Нажмите кнопку «Далее».

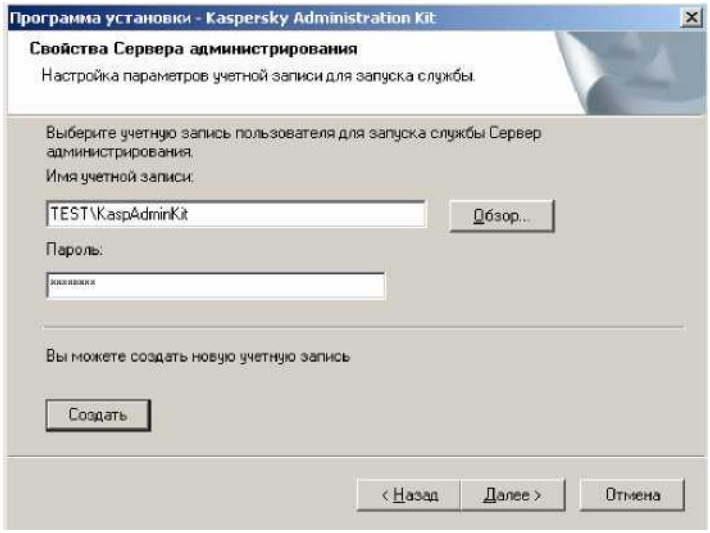


Рис. 5.11. Свойства сервера администрирования На экране появится информационное сообщение о том, какие права будут дополнительно присвоены указанной Вами учетной записи (рис. 5.12). Нажмите кнопку «ОК».

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».

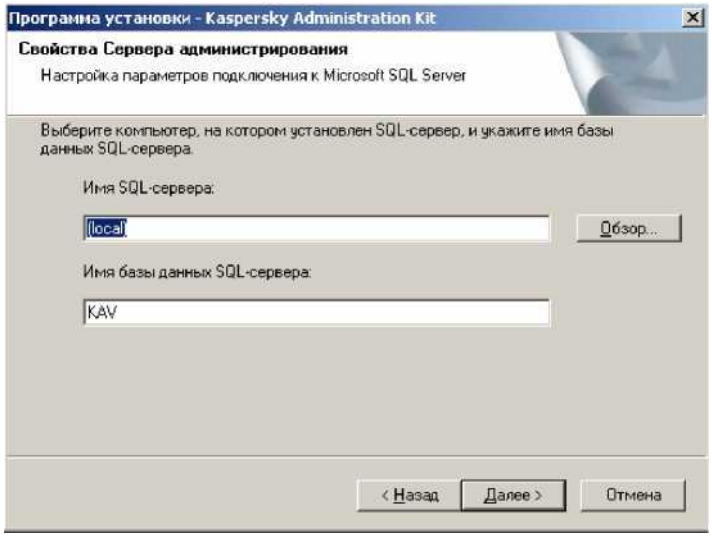


Рис. 5.13. Параметры подключения к MicrosoftSQL-серверу

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

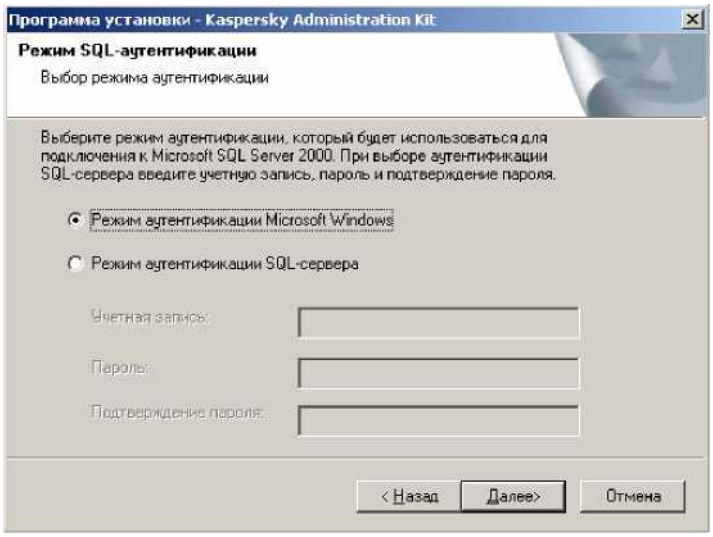


Рис. 5.14. Выбор режима SQL-аутентификации На следующей странице Вам будет предложено указать папку общего доступа для хранения инсталляционных пакетов и обновлений для приложений «Лаборатории Касперского» (рис. 5.15). В этой папке также будет храниться инсталляционный пакет Агента администрирования, 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».

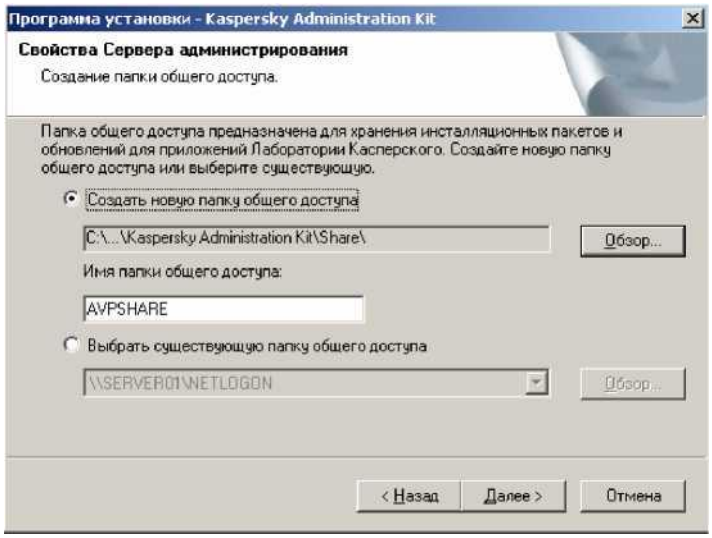


Рис. 5.15. Создание папки общего доступа На следующей странице Вам будет предложено указать номера портов для подключения к Серверу администрирования (рис. 5.16). Если на ком

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».

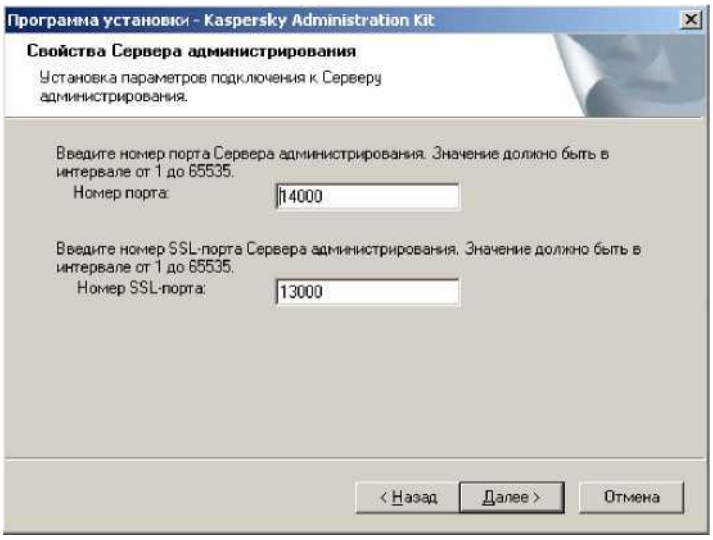


Рис. 5.16. Параметры подключения к Серверу администрирования

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».

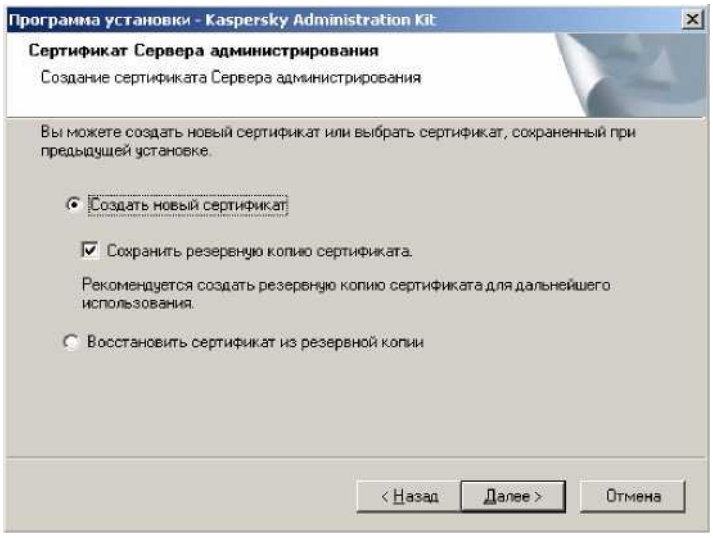


Рис. 5.17. Создание сертификата Сервера администрирования

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».

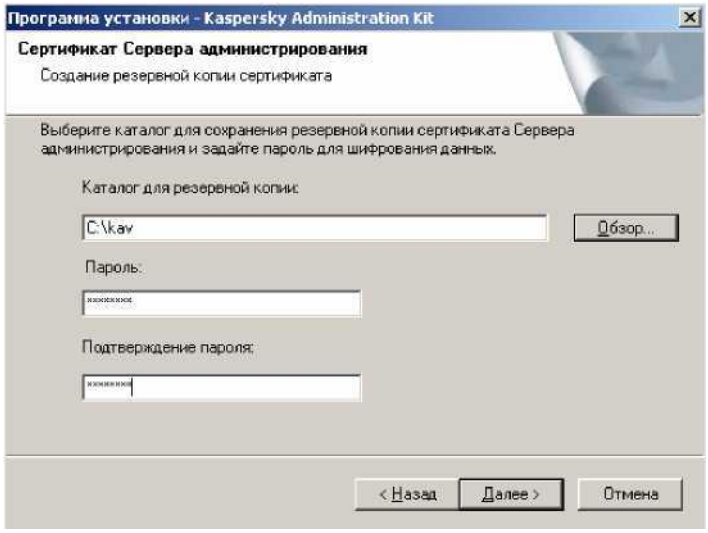


Рис. 5.18. Создание резервной копии сертификата На следующей странице Вам будет предложено ознакомиться с параметрами установки и нажать кнопку «Далее» (рис. 5.19).

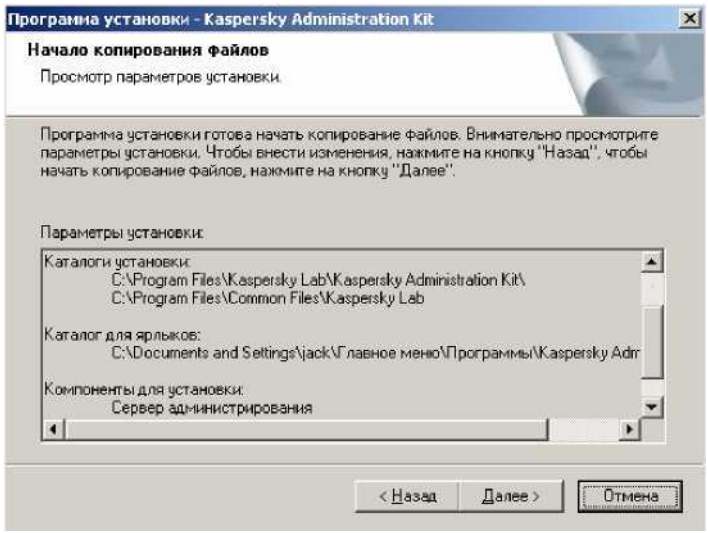


Рис. 5.19. Просмотр параметров установки

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

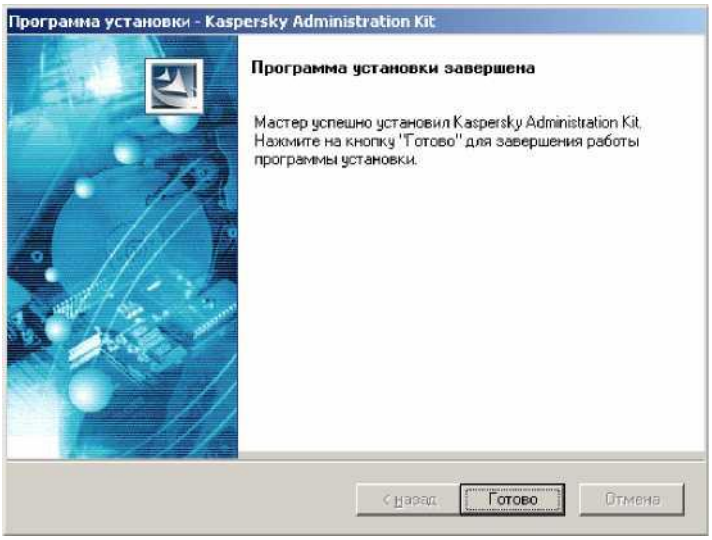


Рис. 5.20. Завершение установки

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».

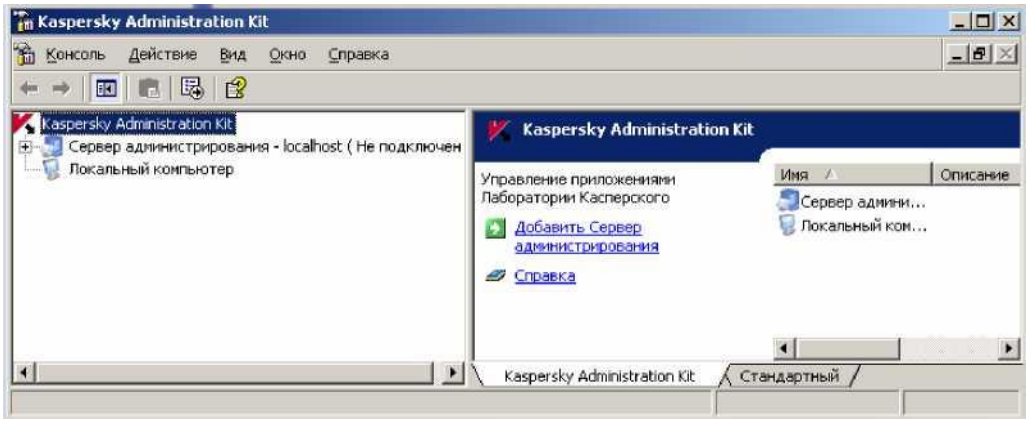


Рис. 5.21. Консоль администрирования

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».

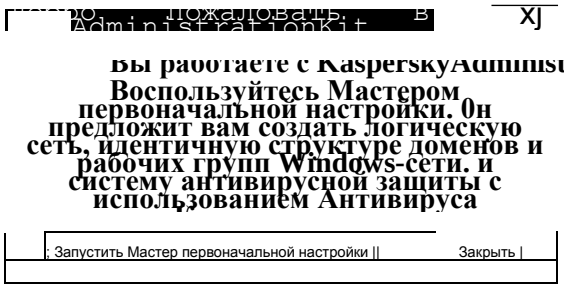


Рис. 5.22. Предложение запустить Мастер первоначальной настройки Мастер первоначальной настройки (рис. 5.23) позволяет сформировать [7]:

- 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.

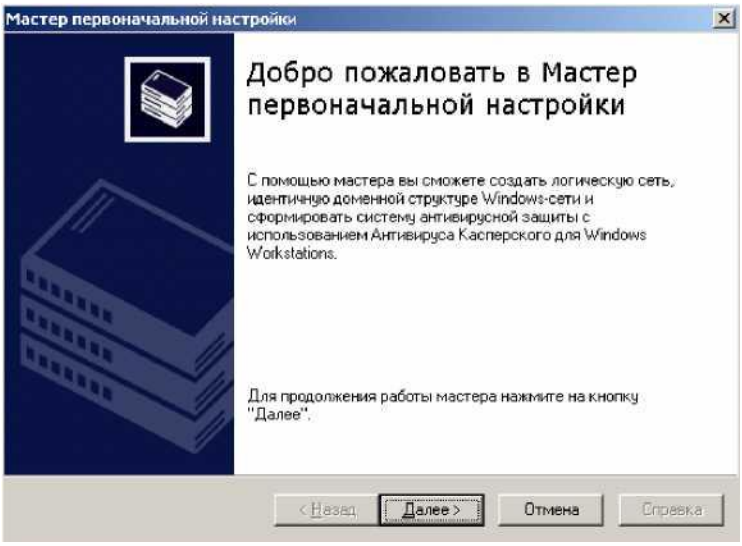


Рис. 5.23. Приветствие Мастера первоначальной настройки Прочитайте приветствие Мастера первоначальной настройки (рис. 5.23) и нажмите кнопку «Далее». Мастер осуществляет опрос сети и на следующей странице отображает сообщение о его завершении (рис. 5.24). Просмотреть результаты опроса сети можно, щелкнув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

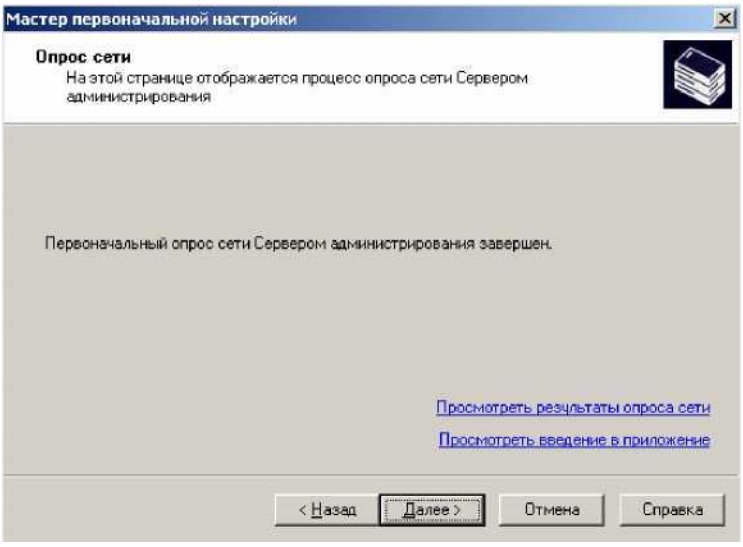


Рис. 5.24. Опрос сети

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».

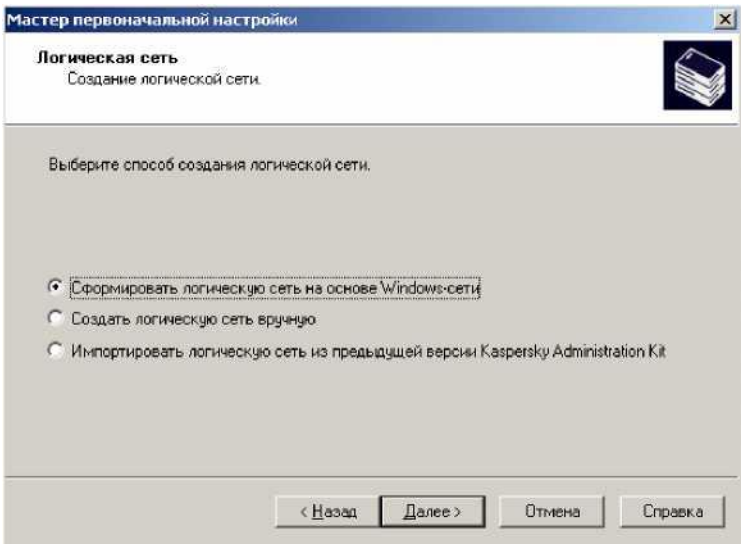


Рис. 5.25. Выбор способа создания логической сетиНа следующей странице Вам будет предложено задать параметры уведомления о событиях, регистрируемых в работе приложений (рис. 5.26). Нажав кнопку «Сообщение» Вы можете отредактировать шаблон отправляемого сообщения. По умолчанию шаблон следующий:

«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».

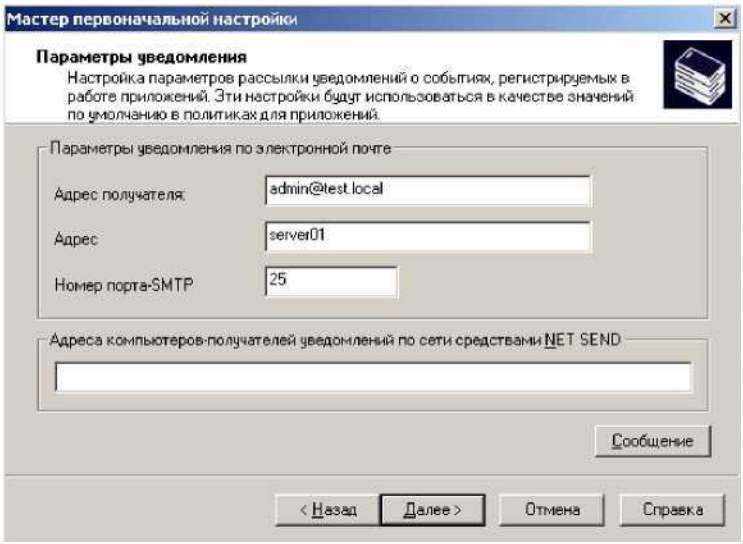


Рис. 5.26. Параметры отправки уведомлений На следующей странице Вам будет сообщено о готовности Мастера к созданию политики и основных групповых задач для Антивируса Касперского для WindowsWorkstationc настройками по умолчанию (рис. 5.27).

Кроме того, будет создана задача получения обновлений Сервером администрирования .

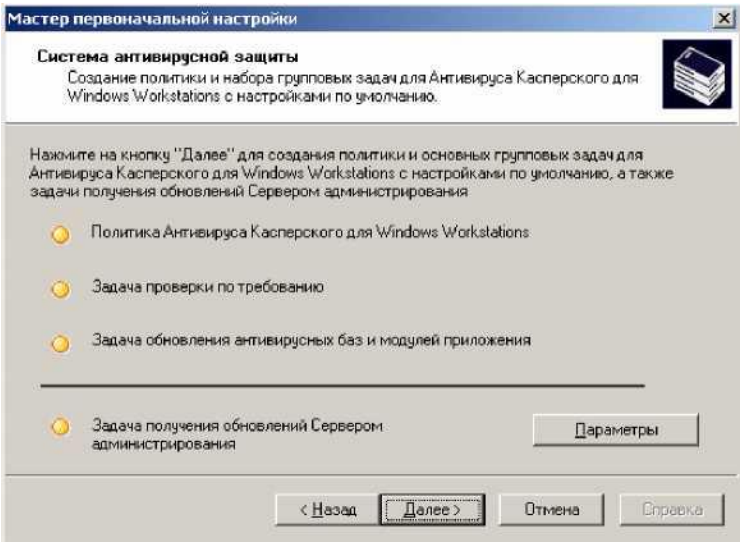


Рис. 5.27. Создание политик и основных групповых задач Нажмите кнопку «Параметры» чтобы задать параметры задачи получения обновлений Сервером администрирования (рис. 5.28). Подробнее о параметрах Вы можете прочитать в документации [7]. Сервер администрирования может получать необходимые Вашей организации 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).

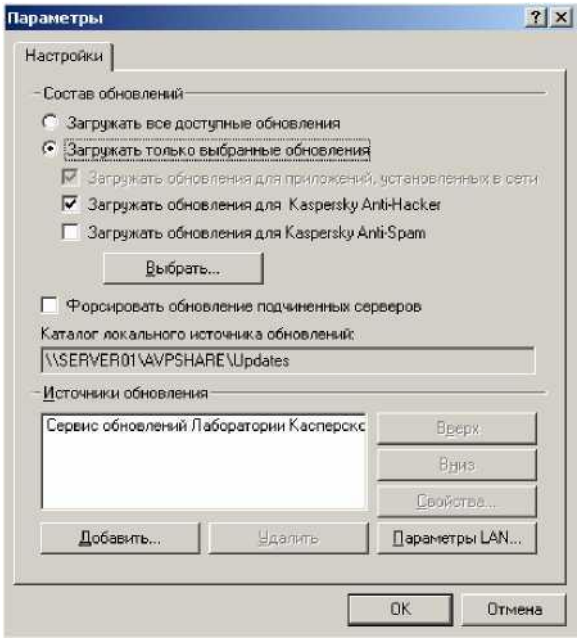


Рис. 5.28. Настройки получения обновлений

Рис. 5.29. Выбор приложений KasperskyAnti-spam

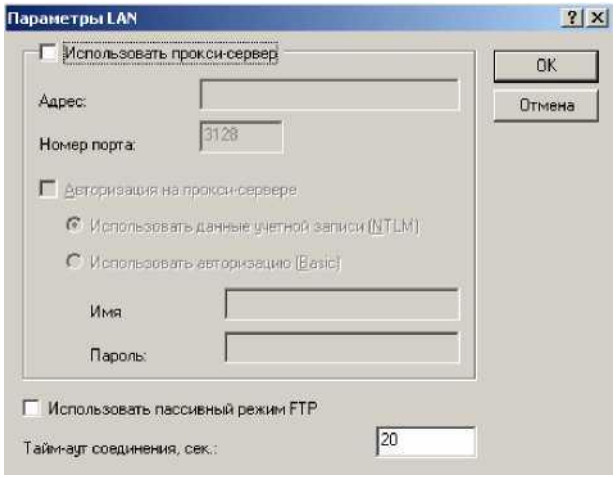


Рис. 5.30. Параметры прокси-сервера

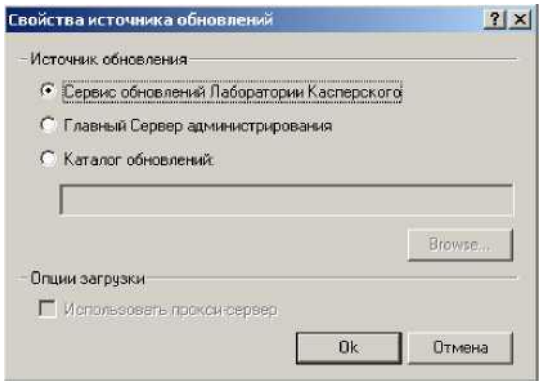


Рис. 5.31. Источники обновления

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)

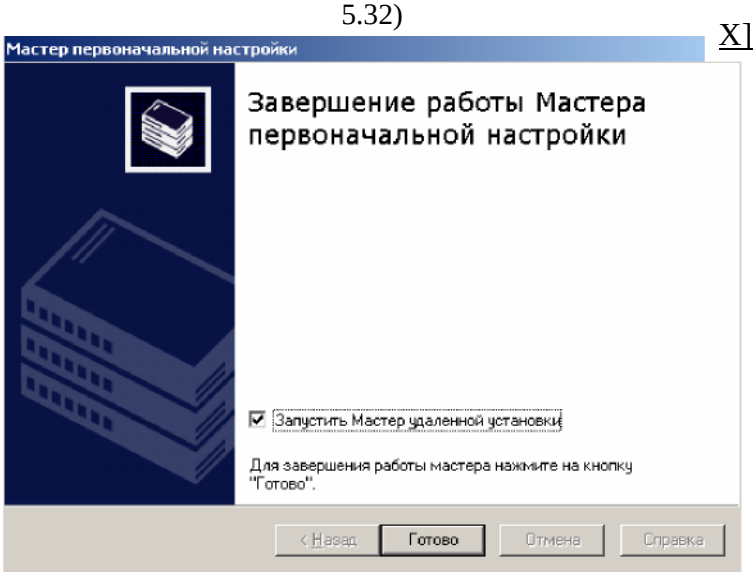


Рис. 5.32. Завершение работы Мастера

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).

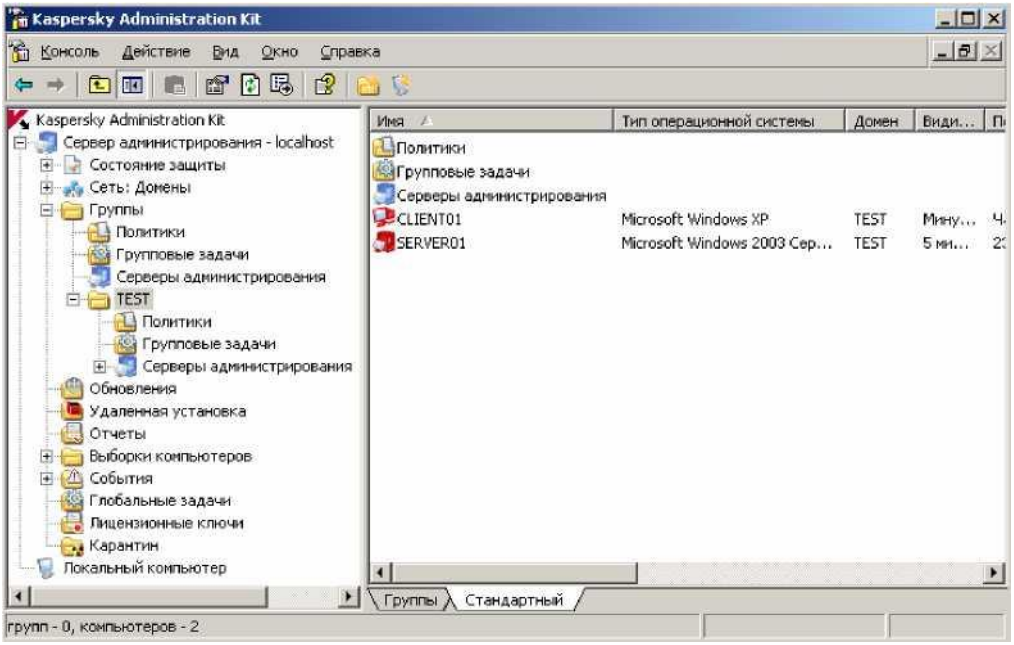


Рис. 5.33. Консоль администрирования

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).

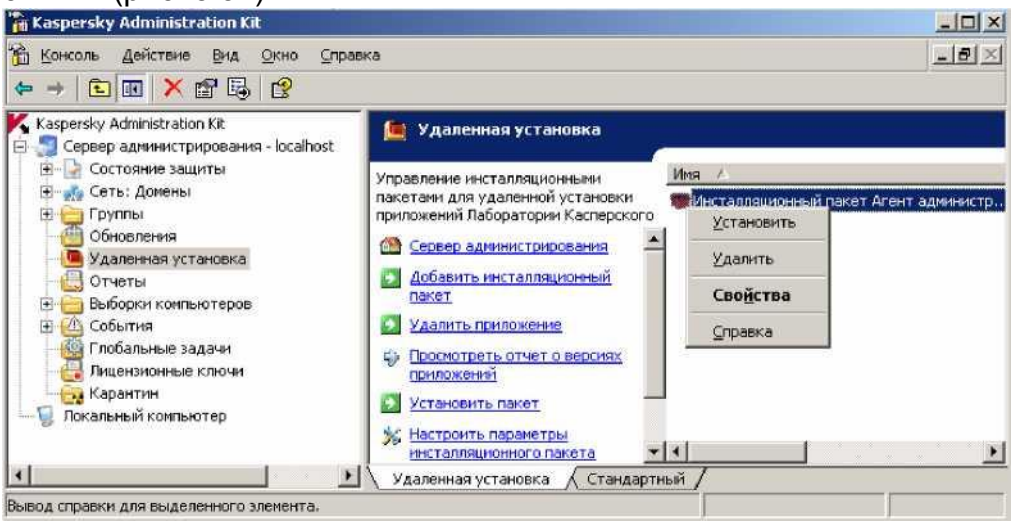


Рис. 5.34. Контекстное меню Удаленной установки Запустится Мастер создания задачи удаленной установки (рис. 5.35). Нажмите кнопку «Далее».

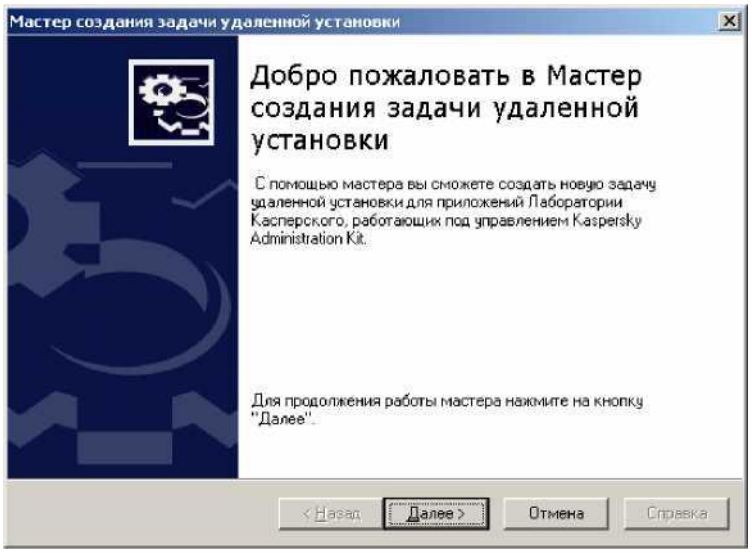


Рис. 5.35. Приветствие Мастера

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

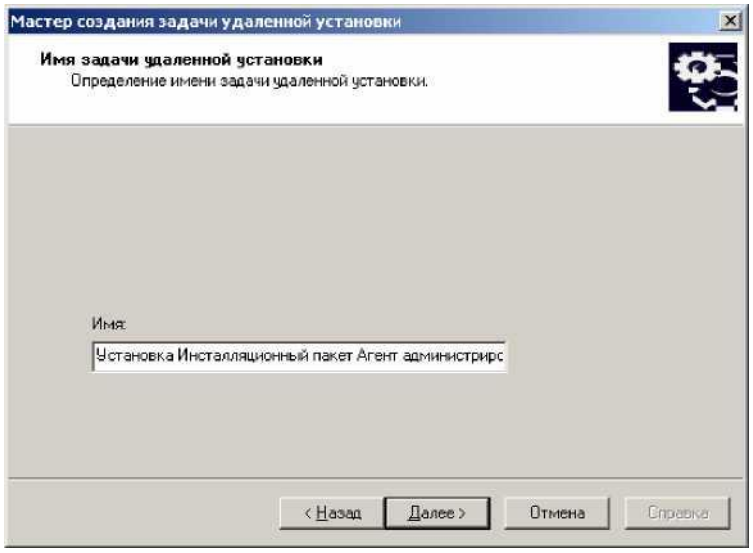


Рис. 5.36. Имя задачи удаленной установки На следующей странице Вам будет предложено выбрать метод удаленной установки (рис. 5.37). Выберите «Форсированная установка» и нажмите кнопку «Далее».

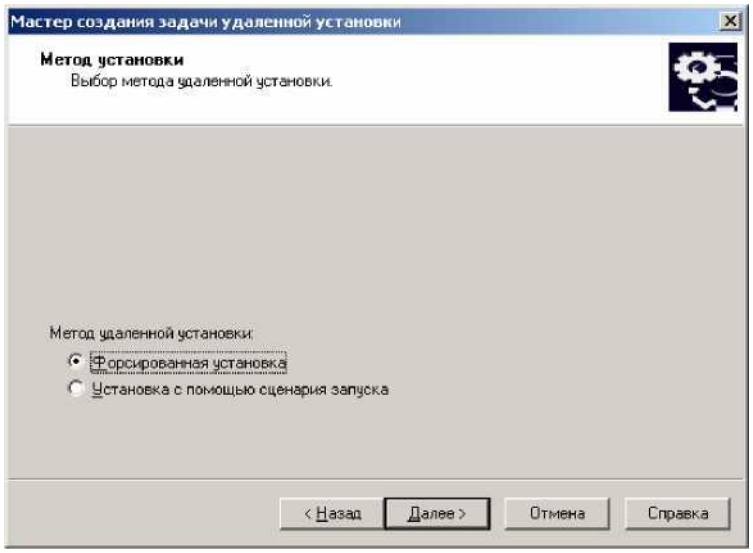


Рис. 5.37. Выбор метода установки

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».

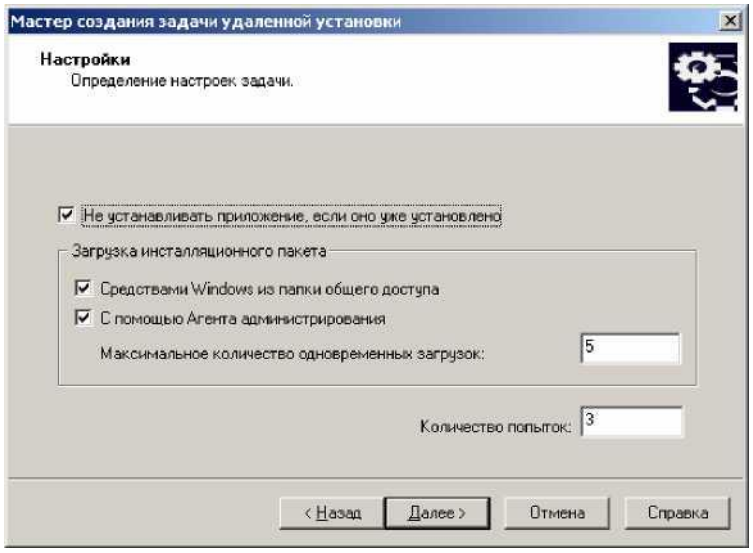


Рис. 5.38. Определение настроек задачи

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».

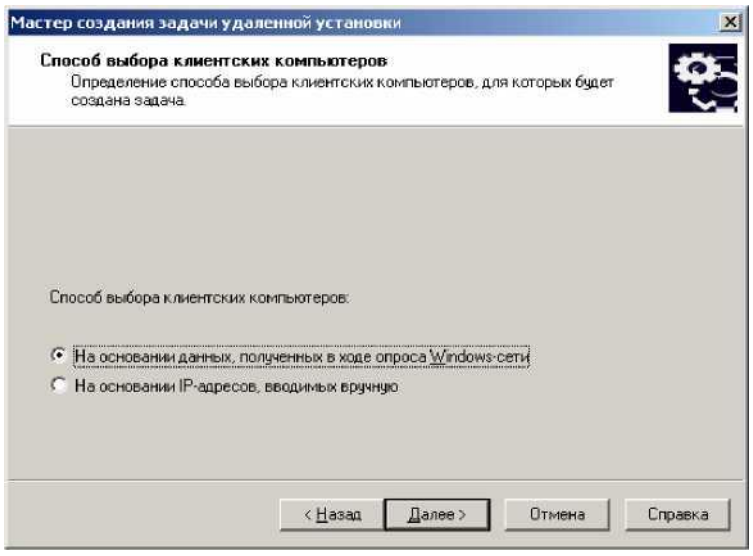


Рис. 5.39. Способ выбора клиентских компьютеров На следующей странице Вам будет предложено определить перечень клиентских компьютеров, на которые будет установлен Агент администрирования (рис. 5.40). Разверните раздел «Группы», отметьте компьютер «Client01» и нажмите кнопку «Далее».

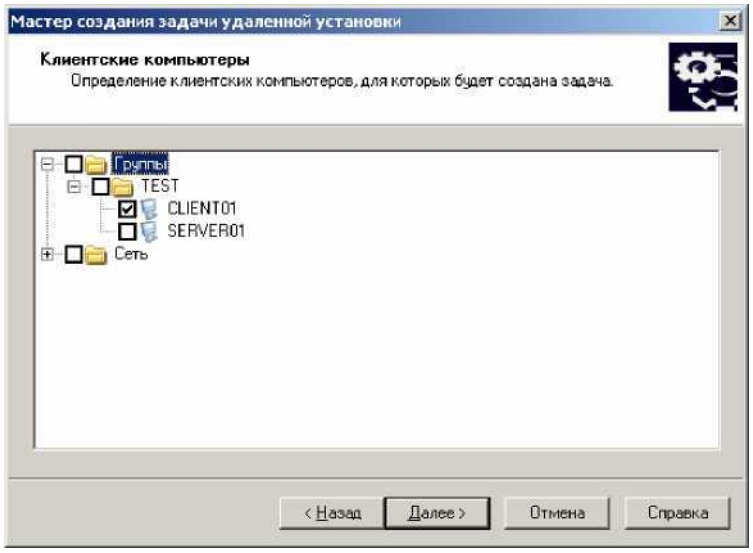


Рис. 5.40. Выбор клиентских компьютеров На следующей странице Вам будет предложено определить учетную запись для запуска создаваемой задачи (рис. 5.41). Если Вы выберите вариант «Учетная запись по умолчанию», то для запуска задачи удаленной установки будет использоваться учетная запись, под которой выполняется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

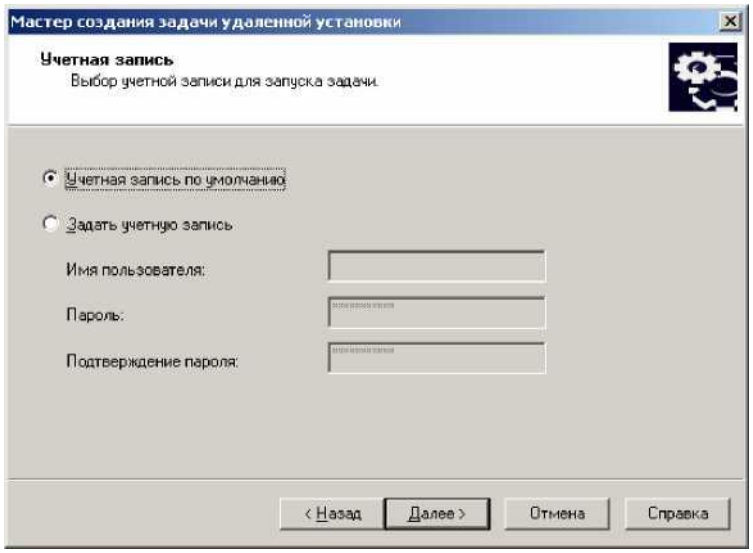


Рис. 5.41. Выбор учетной записи для запуска задачи На следующей странице Вам будет предложено определить расписание для запуска создаваемой задачи (рис. 5.42). На рисунке представлены доступные варианты. Выберите вариант «Немедленно» и нажмите кнопку «Далее».

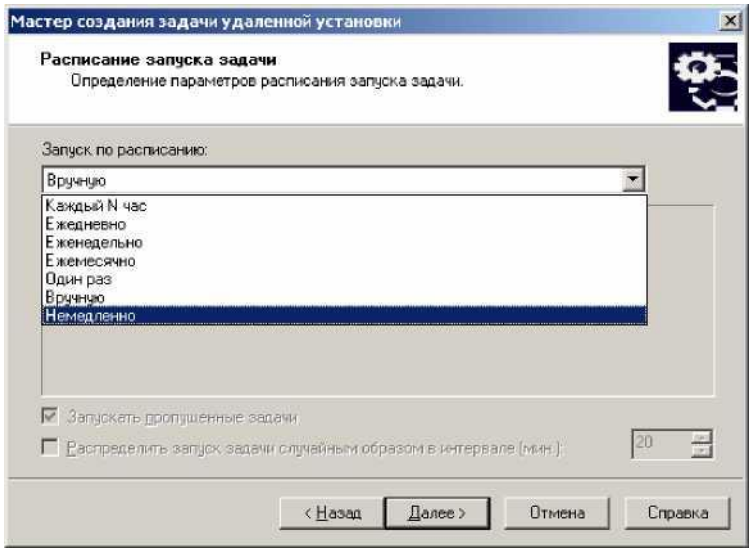


Рис. 5.42. Расписание запуска задачи На следующей странице (рис. 5.43) нажмите кнопку «Далее».

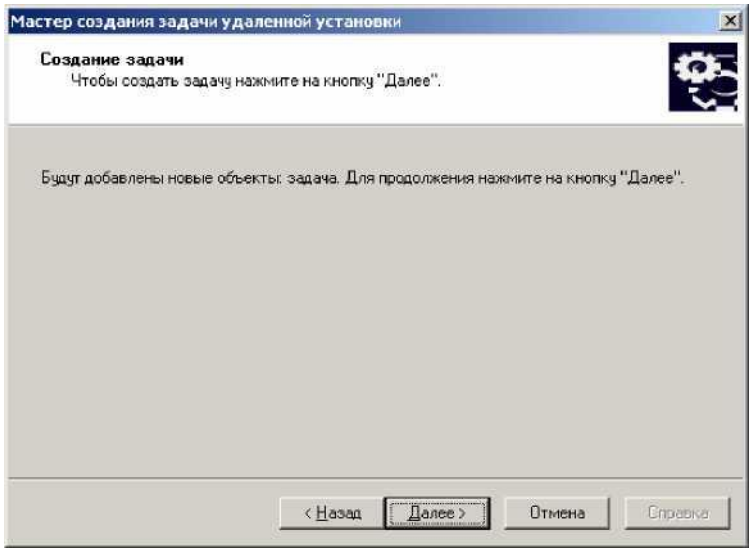


Рис. 5.43. Создание задачи

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

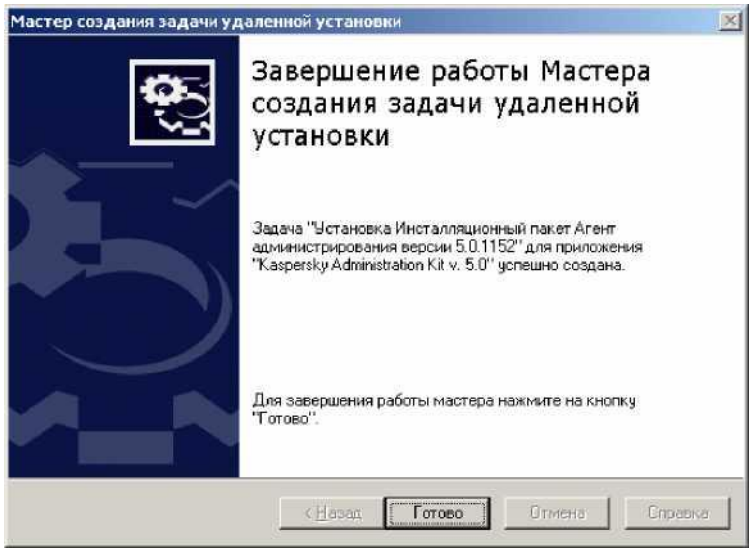


Рис. 5.44. Завершение работы Мастера

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 &.

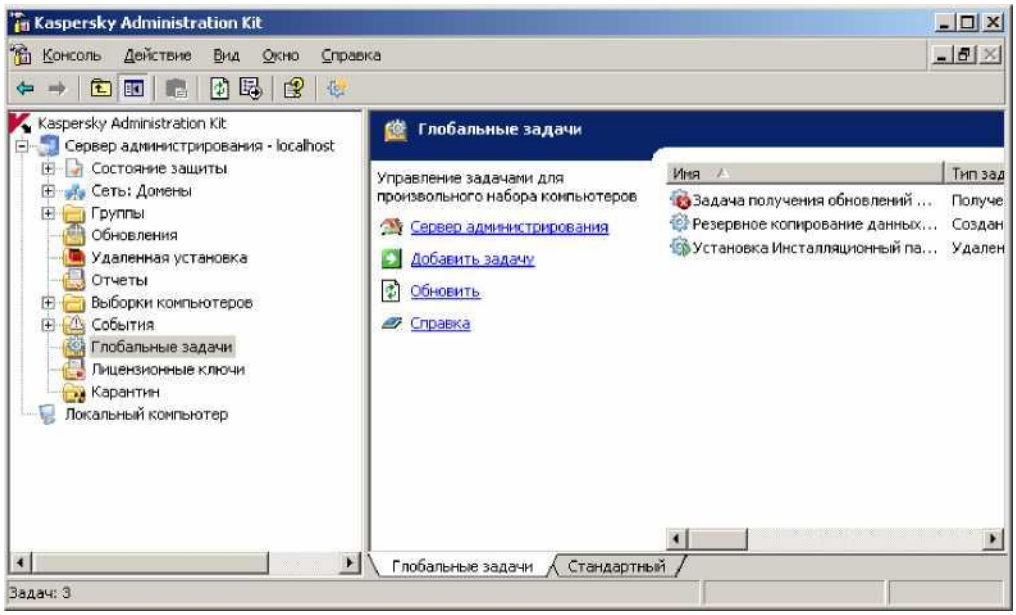


Рис. 5.45. Глобальные задачи

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

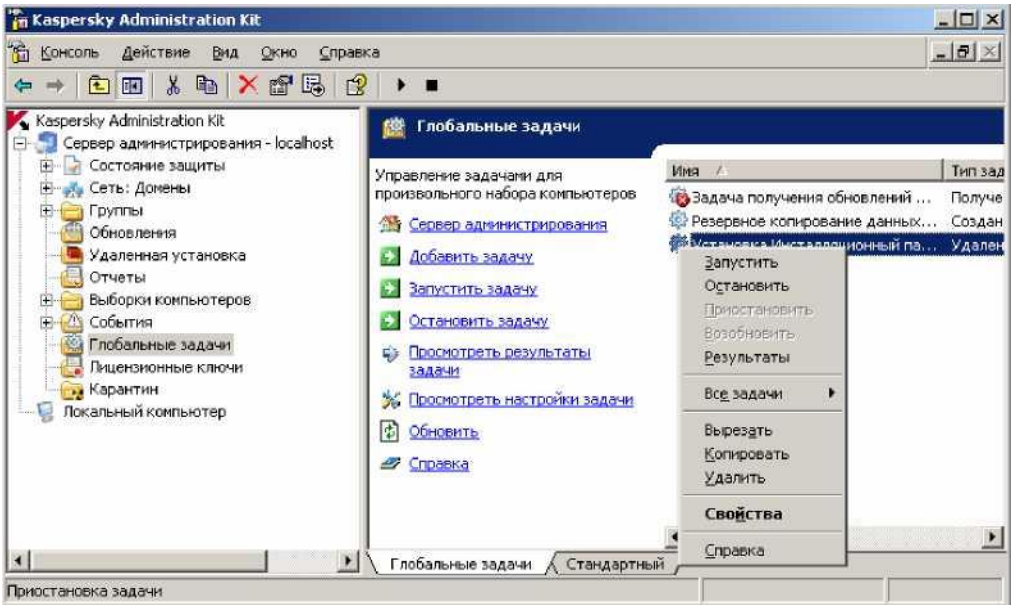


Рис. 5.46. Контекстное меню задачи

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).

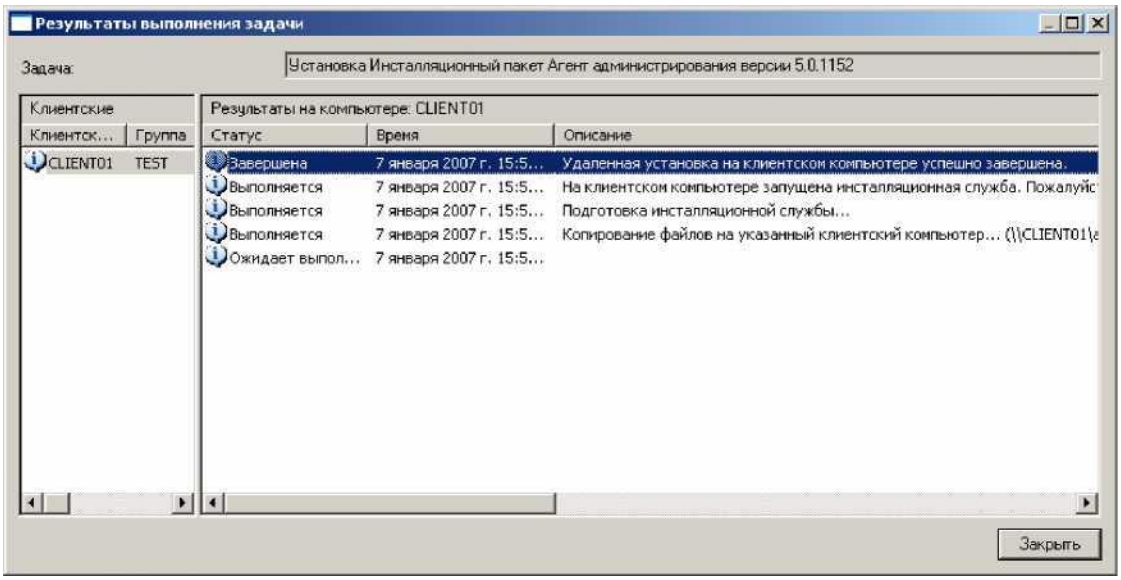


Рис. 5.47. Результаты выполнения задачи

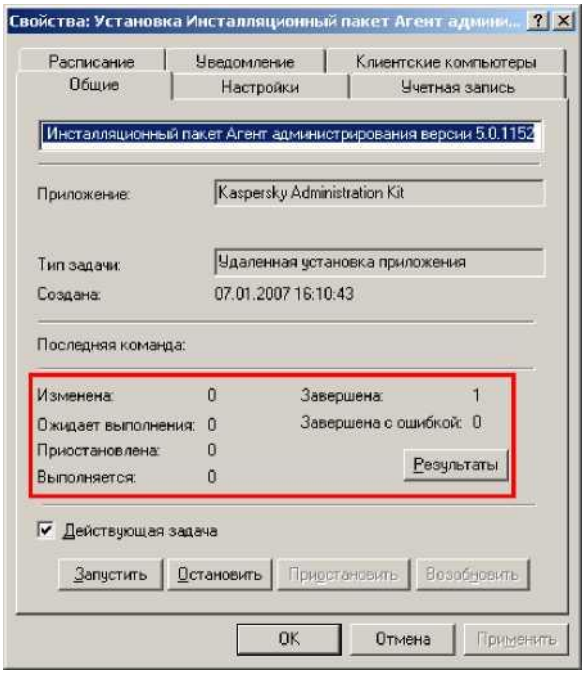


Рис. 5.48. Окно свойств задачи

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).

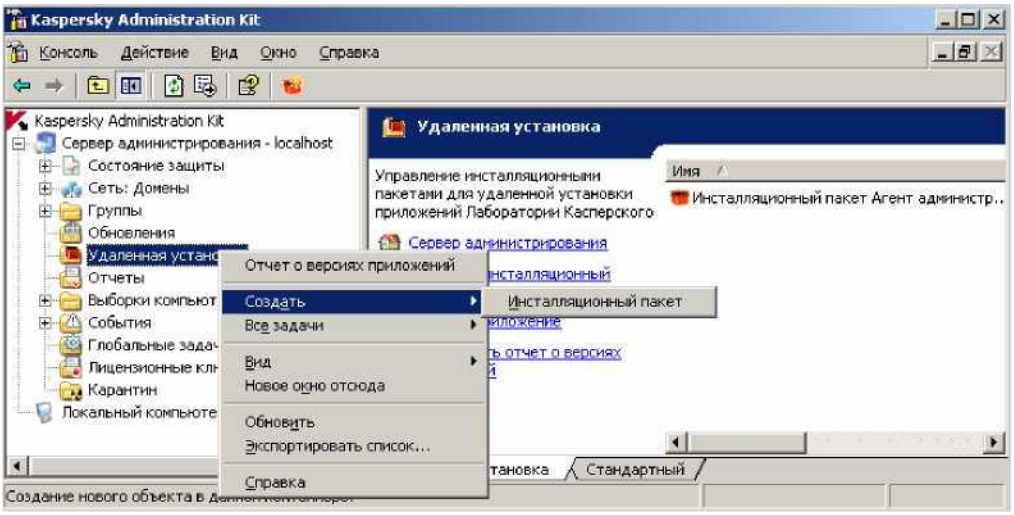


Рис. 5.49. Контекстное меню Удаленной установки Запустится Мастер создания инсталляционного пакета (рис. 5.50). Нажмите кнопку «Далее».

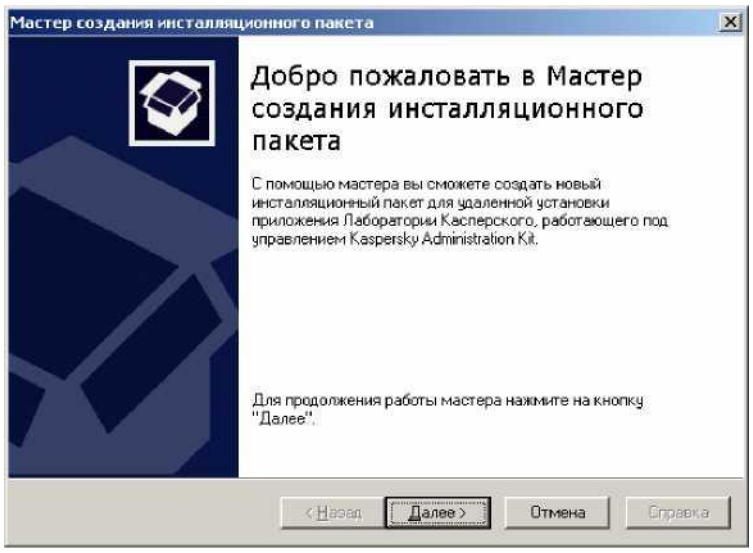


Рис. 5.50. Мастер создания инсталляционного пакета На следующей странице Вам будет предложено задать имя создаваемого инсталляционного пакета (рис. 5.51). Введите имя (например, «Инсталляционный пакет Антивирус Касперского для WindowsWorkstation») и нажмите кнопку «Далее».

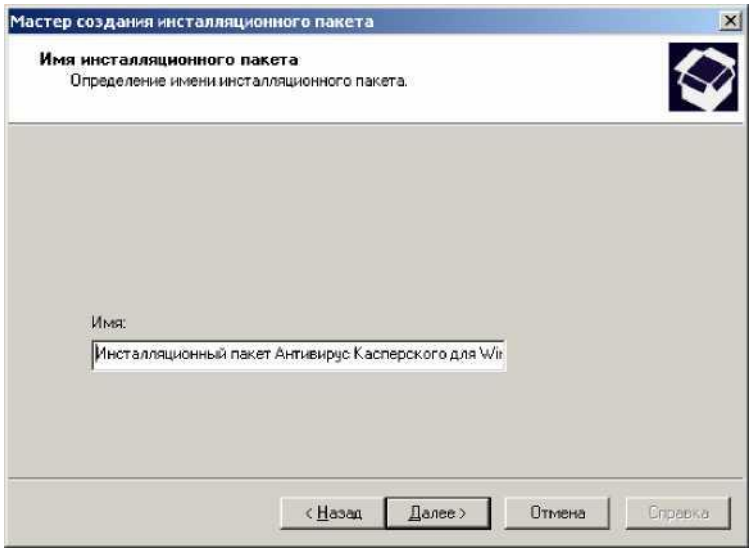


Рис. 5.51. Имя инсталляционного пакета

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».

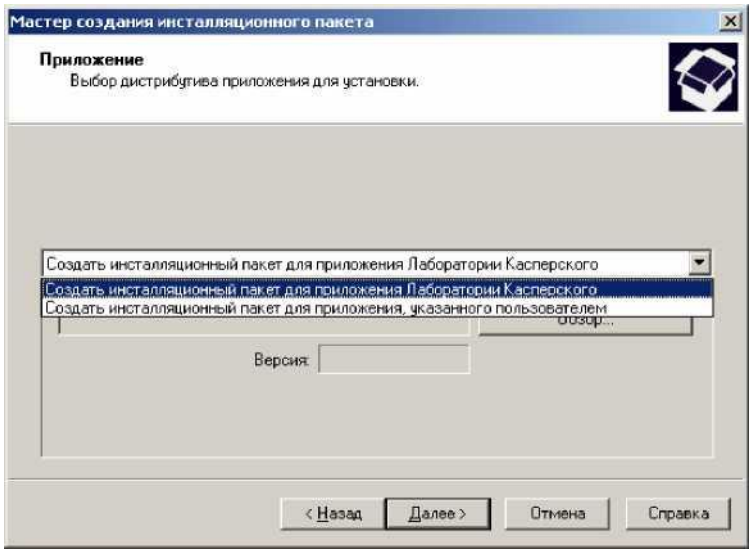


Рис. 5.52. Выбор дистрибутива продукта

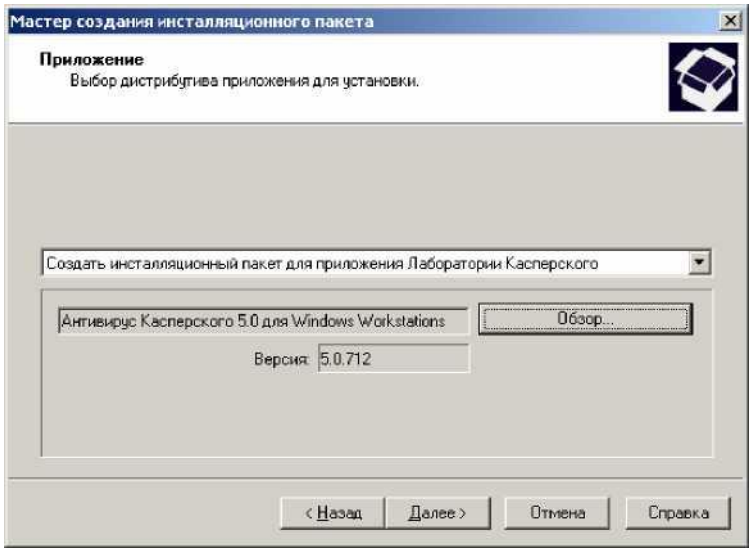


Рис. 5.53. После указания файла .kpd

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».

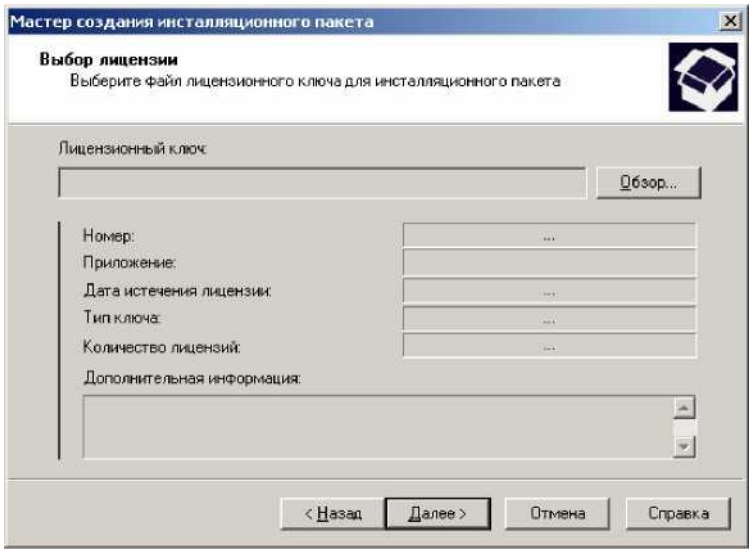


Рис. 5.54. Выбор лицензии

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 KasperskyAdministrationKit[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».

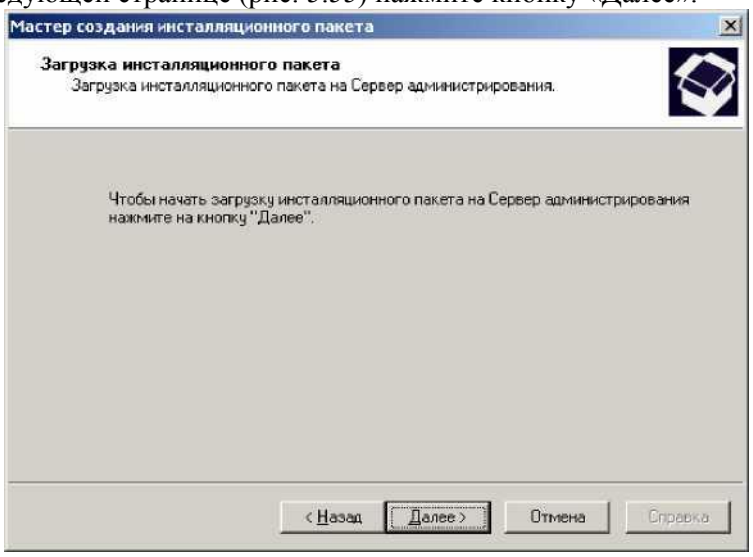


Рис. 5.55. Загрузка инсталляционного пакета Если во время загрузки инсталляционного пакета появится предупреждение, показанное на рис. 5.56, нажмите кнопку «Открыть» и загрузка будет продолжена.

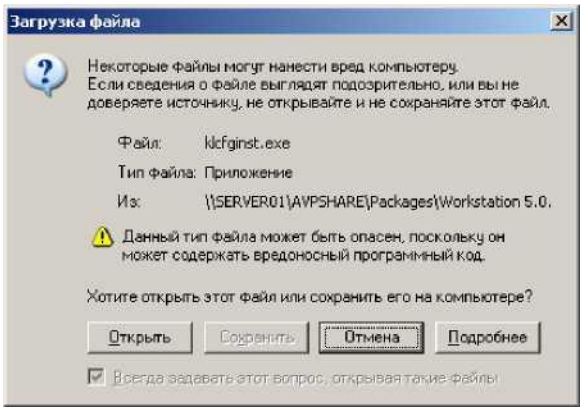


Рис. 5.56. Предупреждение ОС

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

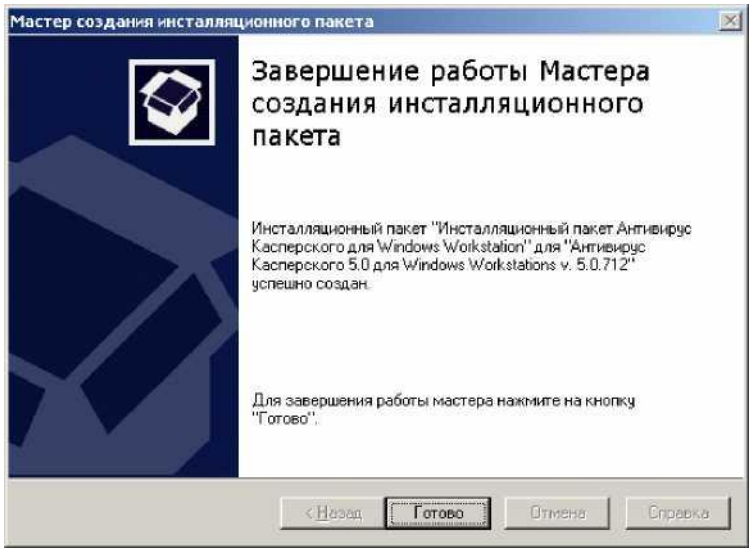


Рис. 5.57. Завершение работы Мастера

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.

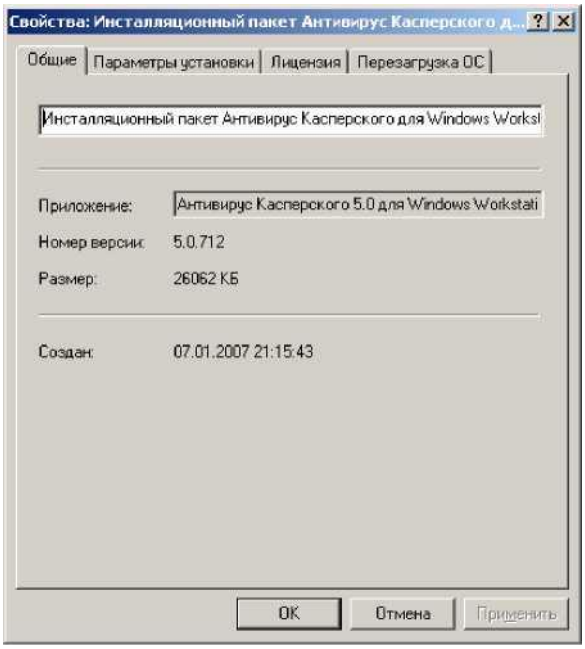


Рис. 5.58. Страница Общие

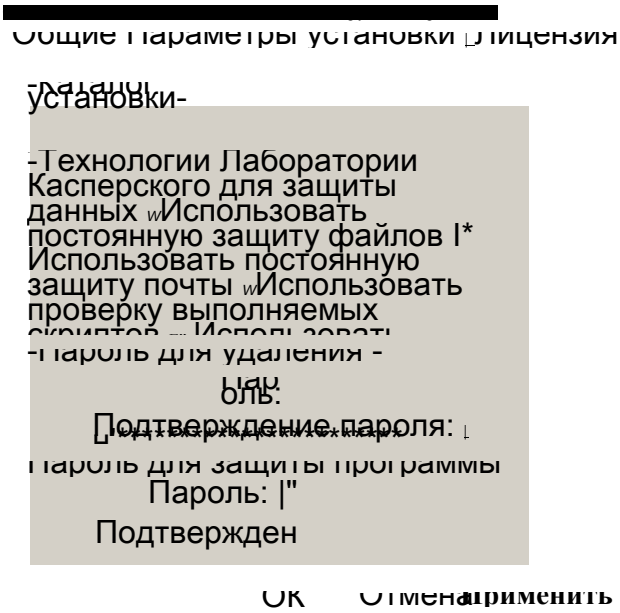


Рис. 5.59. Страница Параметры установки

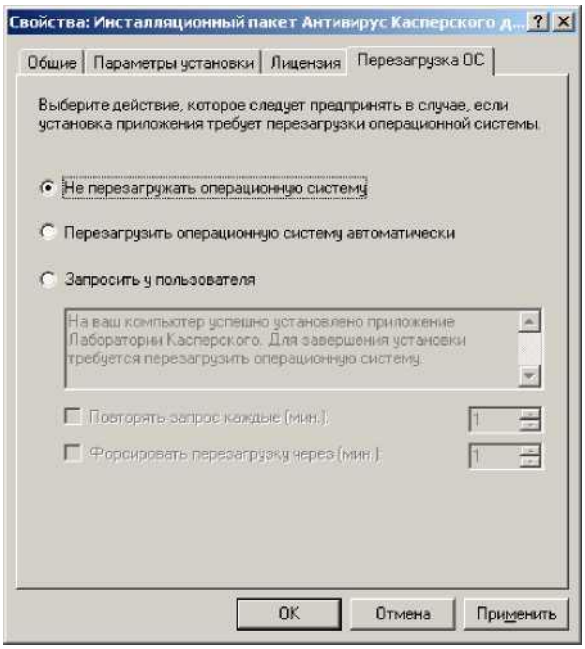


Рис. 5.60. Страница Перезагрузка ОС

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.

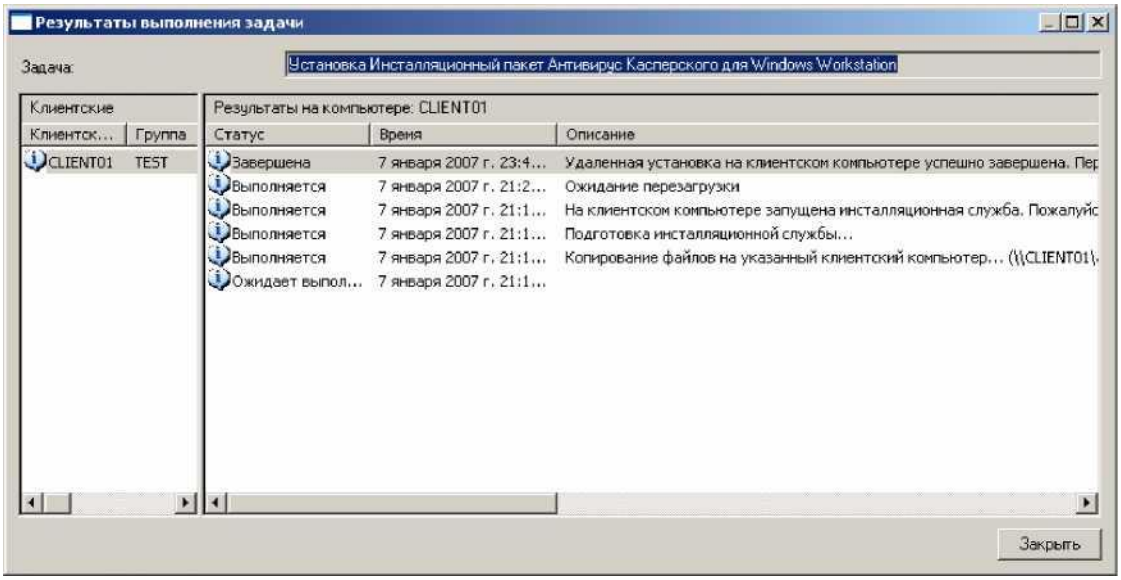


Рис. 5.61. Результаты выполнения задачи

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.

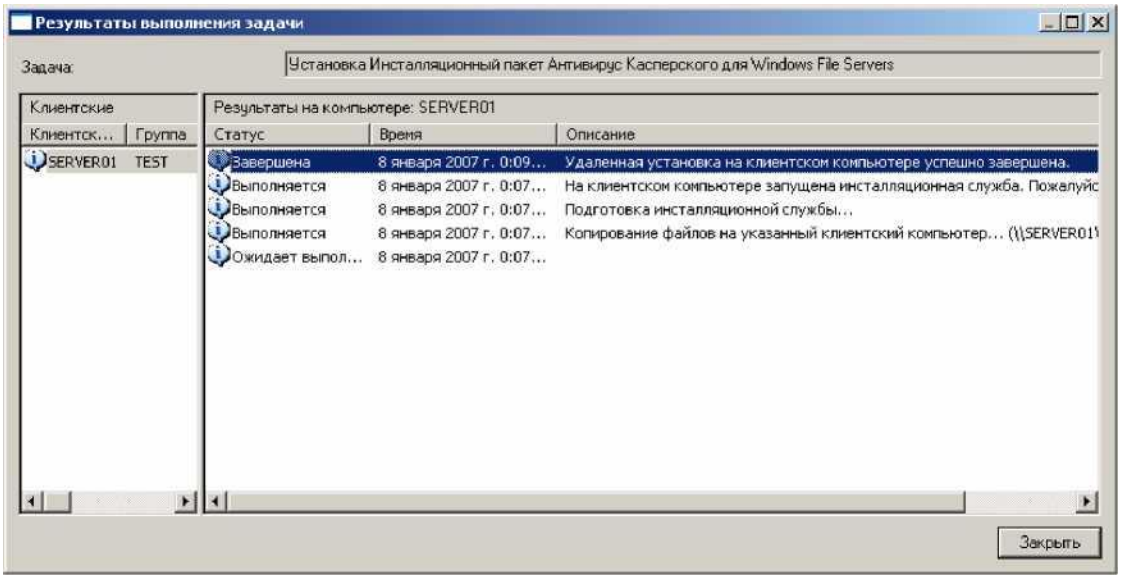


Рис. 5.62. Результаты выполнения задачи

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.

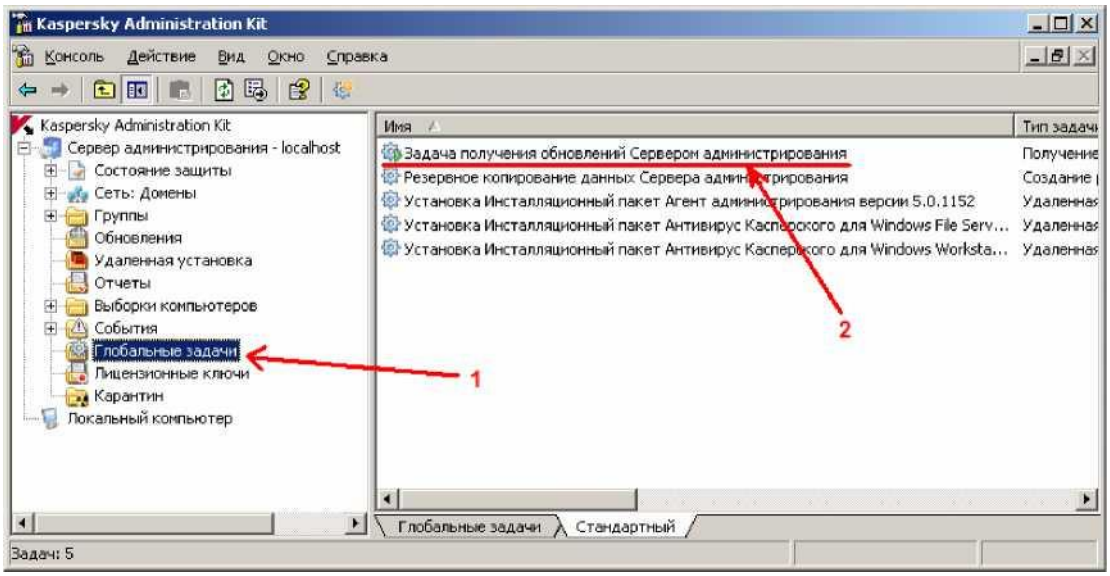


Рис. 5.63. Задача получения обновлений Сервером администрирования

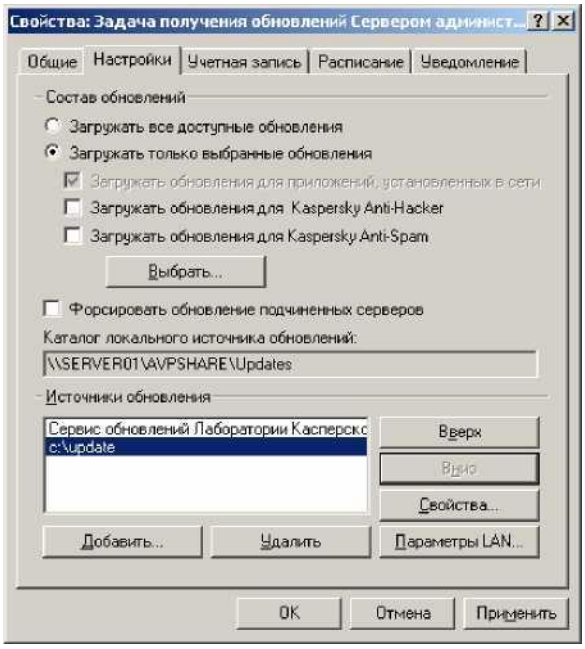


Рис. 5.64. Страница Настройки

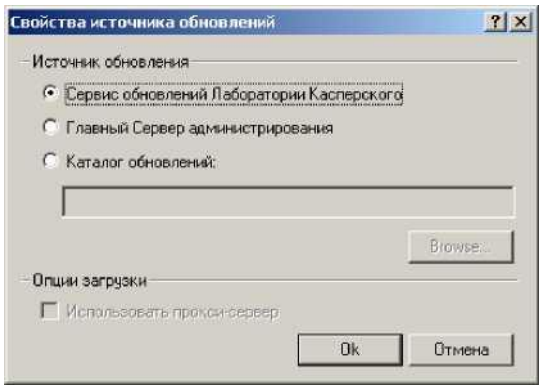


Рис. 5.65. Источники обновления

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].

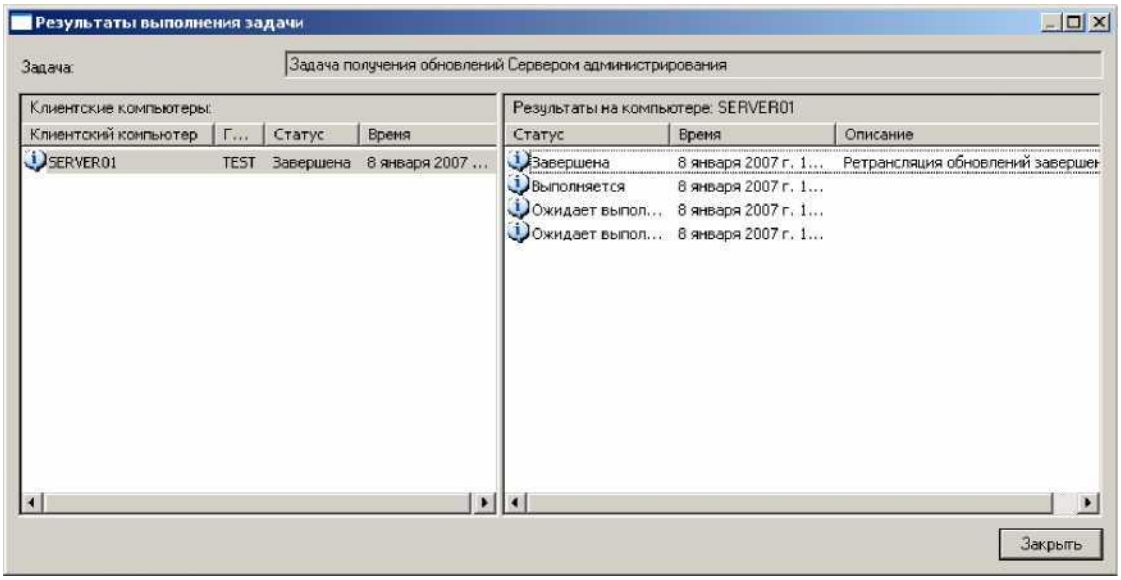


Рис. 5.66. Результаты выполнения задачи

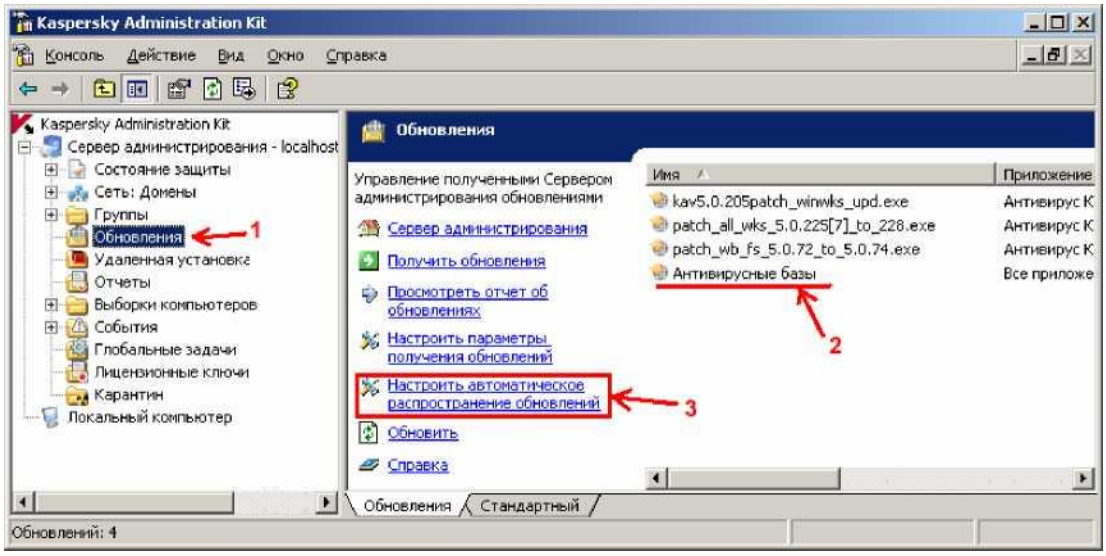


Рис. 5.67. Узел Обновления

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.

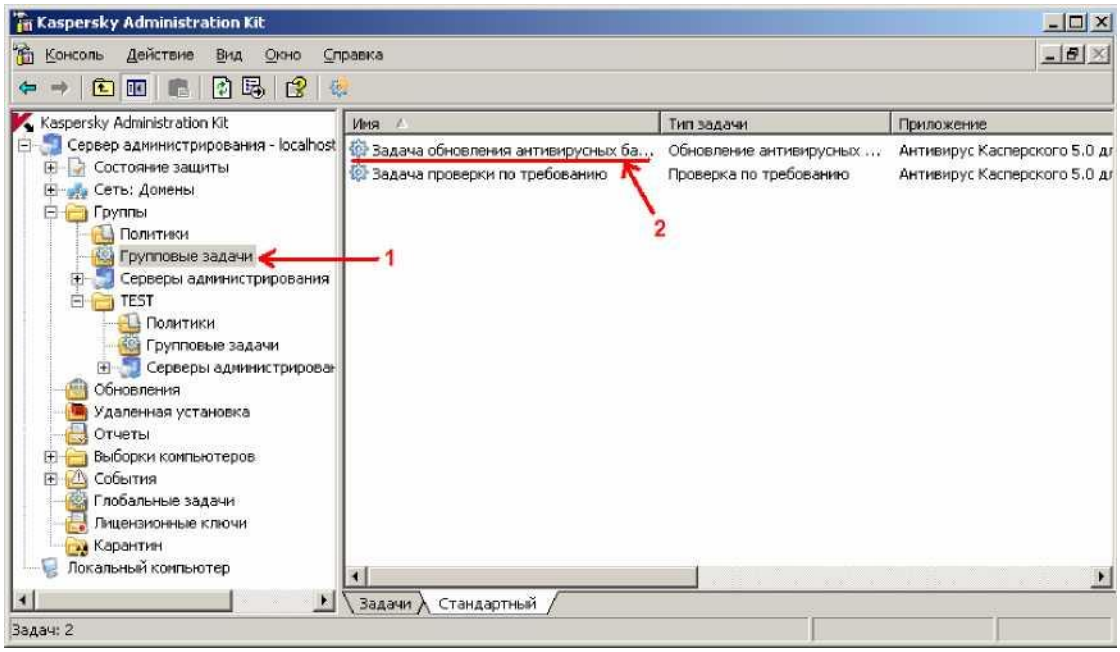


Рис. 5.68. Задача обновления антивирусных баз На рис. 5.69 представлена закладка «Настройки» окна свойств этой задачи. Если в Вашей организации обновление клиентских станций будет осуществляться только с Сервера администрирования, то в этом окне можно отключить источник обновления «Серверы обновлений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

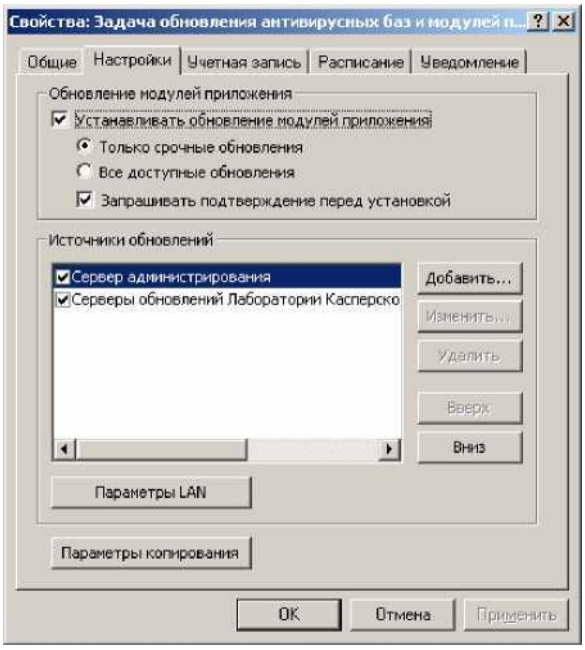


Рис. 5.69. Страница Настройки

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».

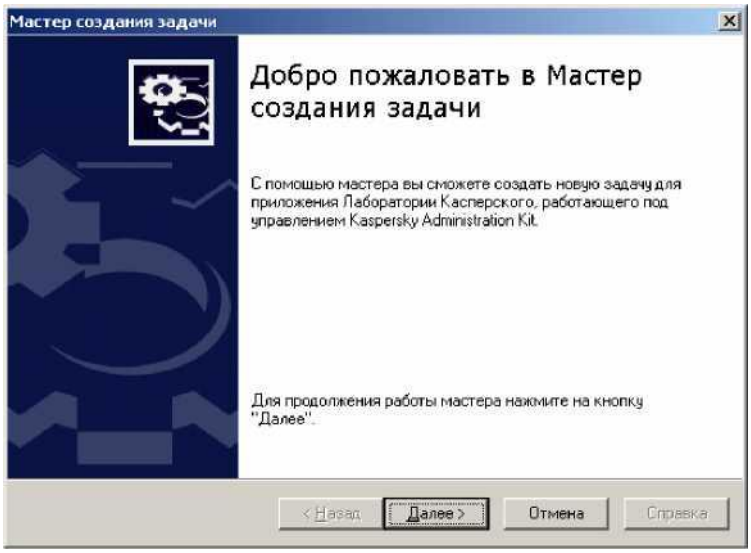


Рис. 5.70. Приветствие Мастера

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

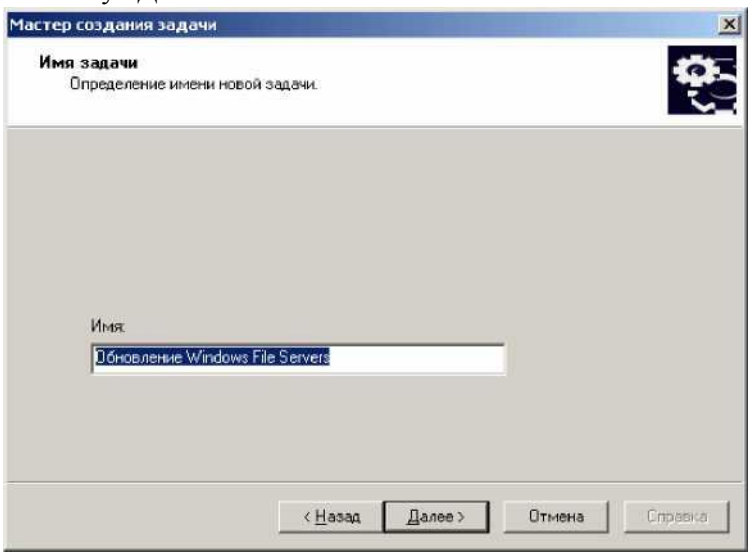


Рис. 5.71. Имя задачи

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».

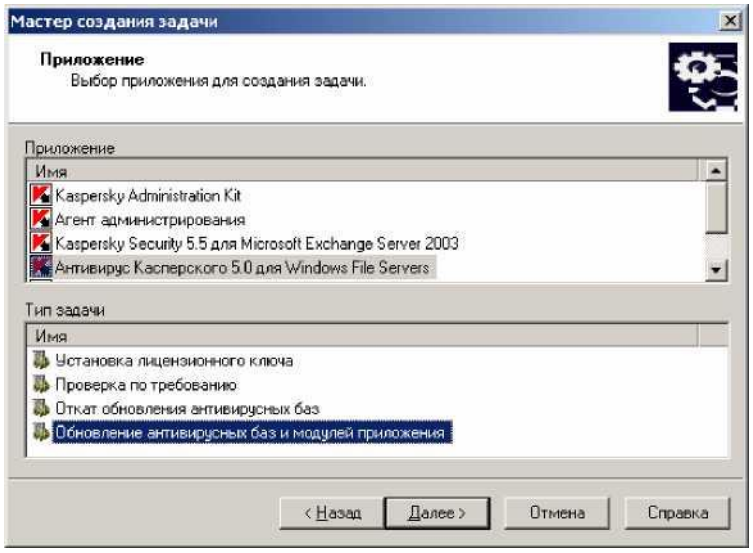


Рис. 5.72. Выбор приложения и типа задачи На следующей странице Вам будет предложено выбрать источник обновления (рис. 5.73). Выберите «Сервер администрирования» и нажмите кнопку «Далее».

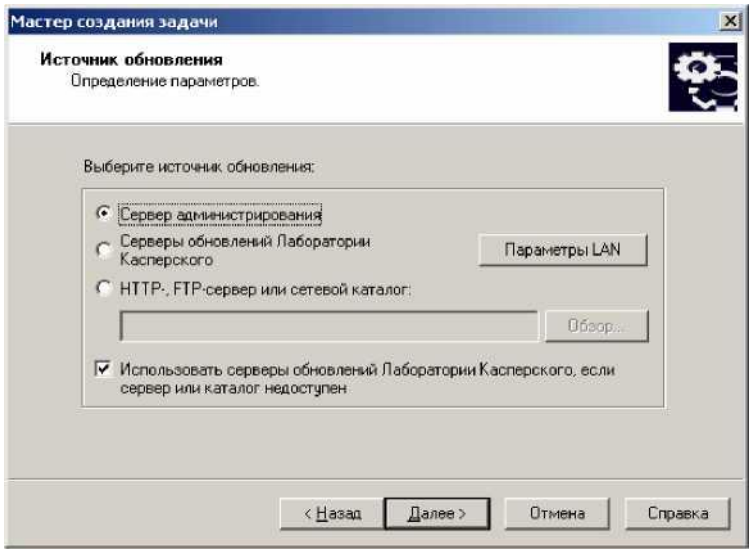


Рис. 5.73. Выбор источника обновления

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».

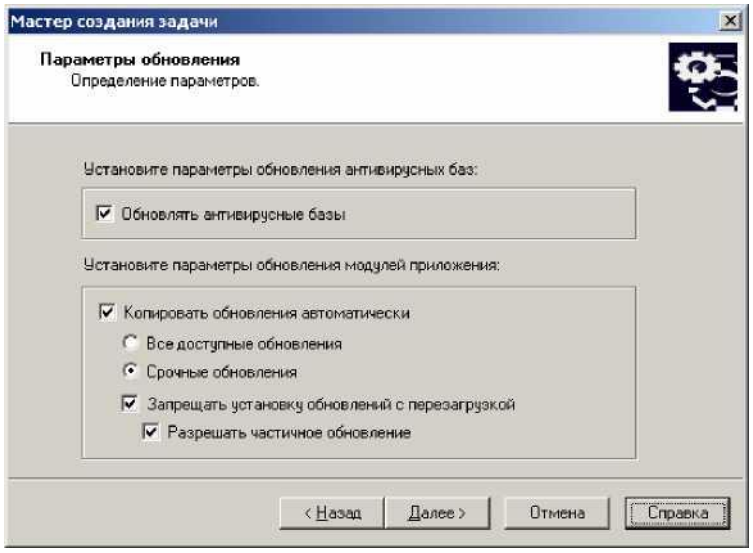


Рис. 5.74. Параметры обновления

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

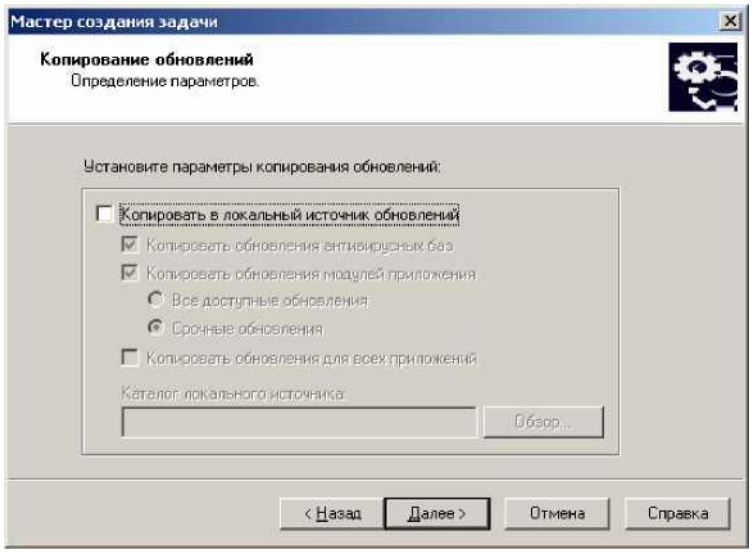


Рис. 5.75. Копирование обновлений

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

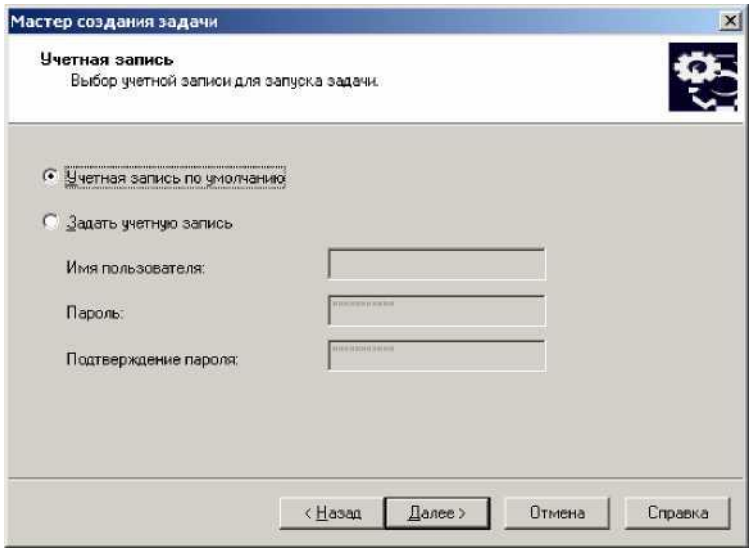


Рис. 5.76. Выбор учетной записи

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».

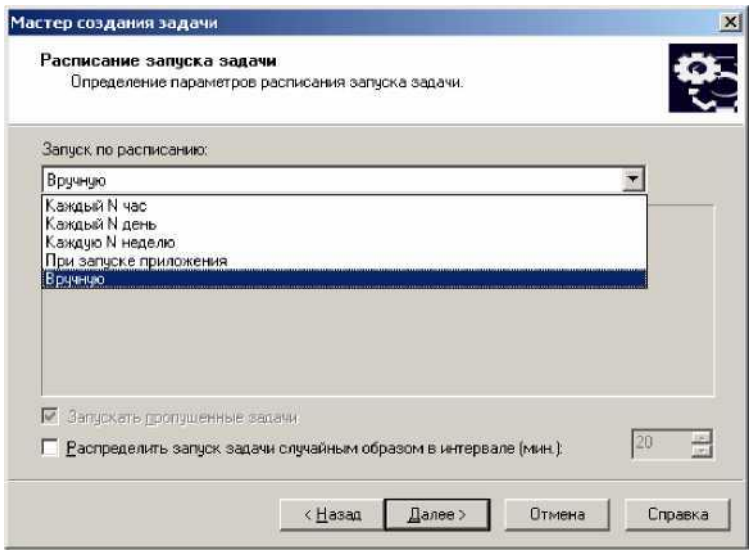


Рис. 5.77. Расписание запуска задачи На следующей странице (рис. 5.78) нажмите кнопку «Далее».

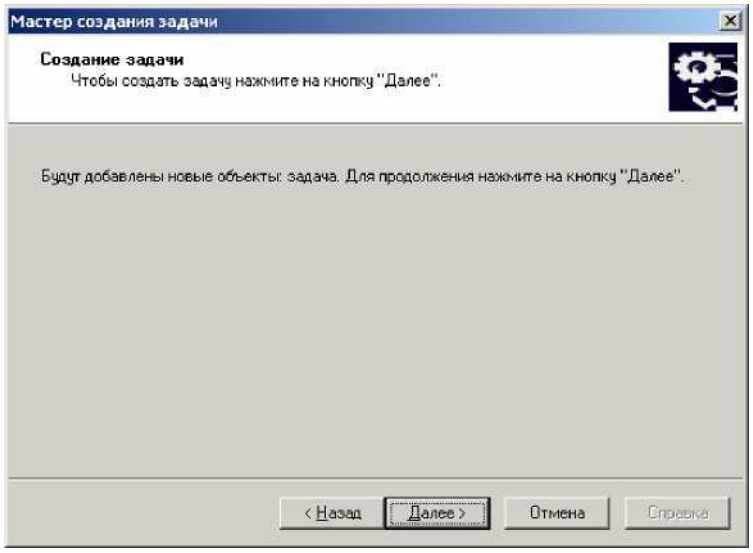


Рис. 5.78. Создание задачи

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

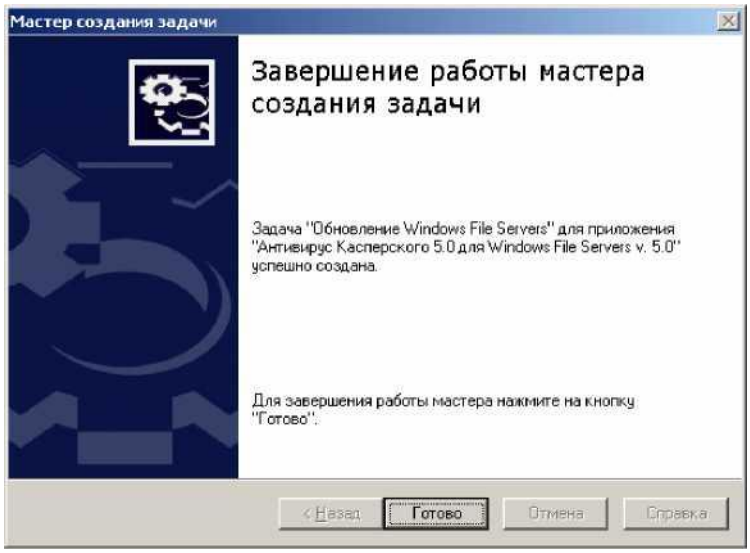


Рис. 5.79. Завершение работы Мастера

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).

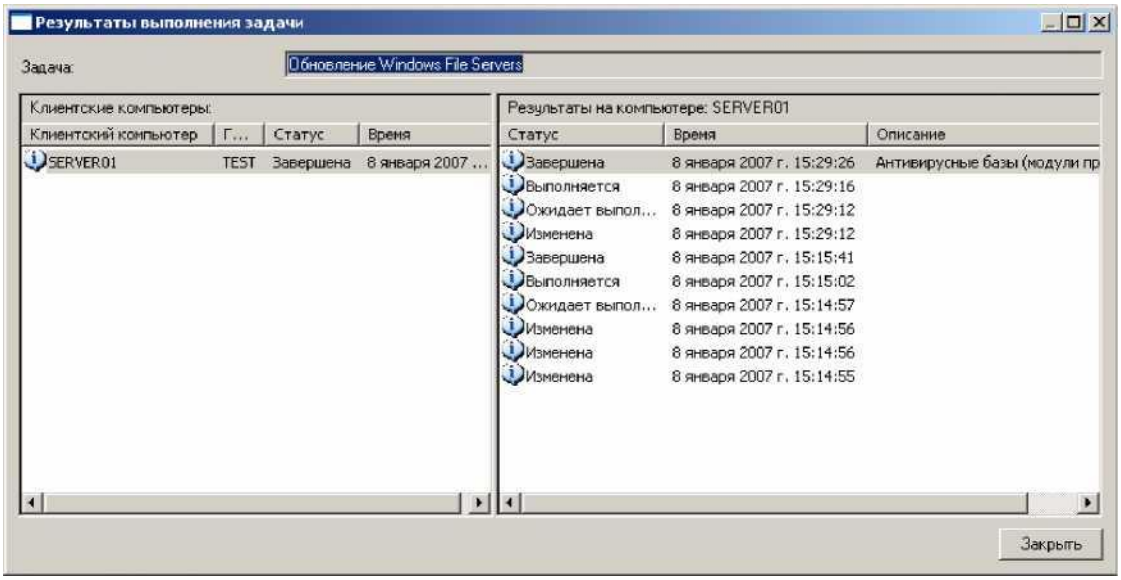


Рис. 5.80. Результаты выполнения задачи

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).

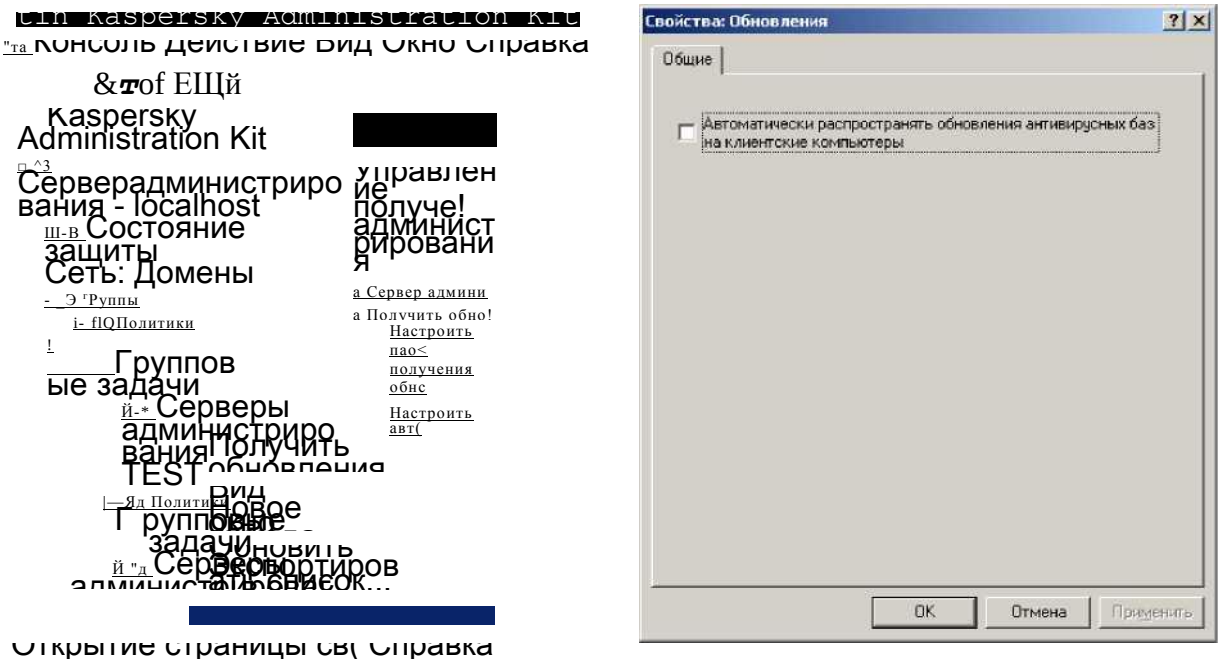


Рис. 5.81. Свойства узла Обновления

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].

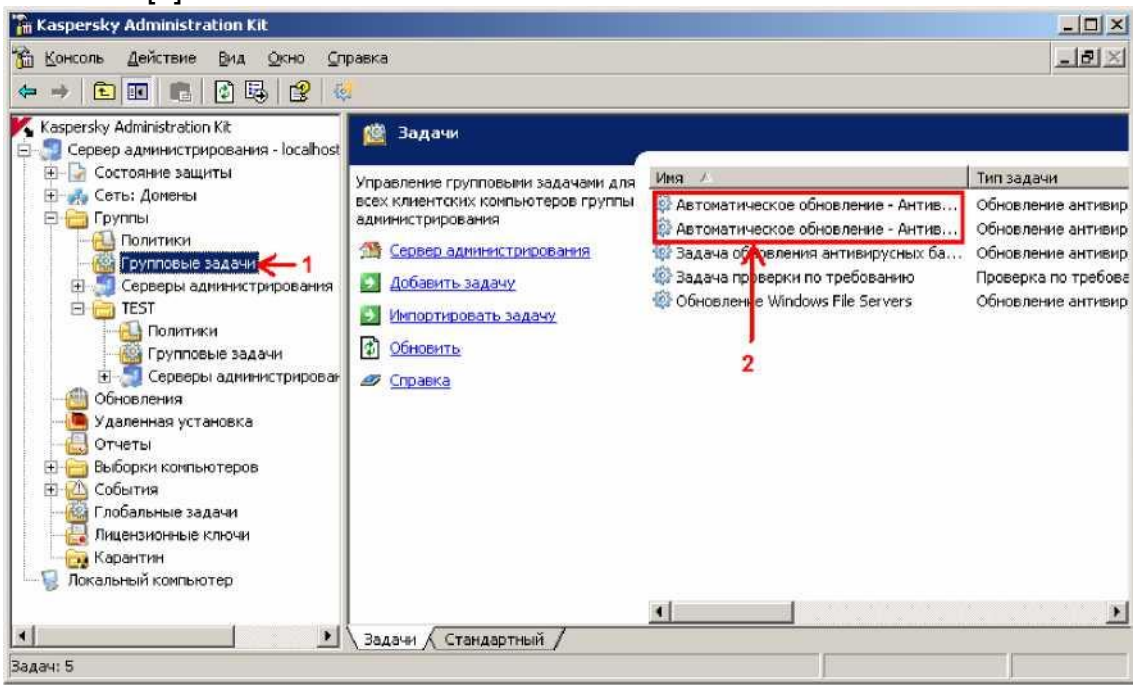


Рис. 5.82. Задачи автоматического распространения обновлений

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).

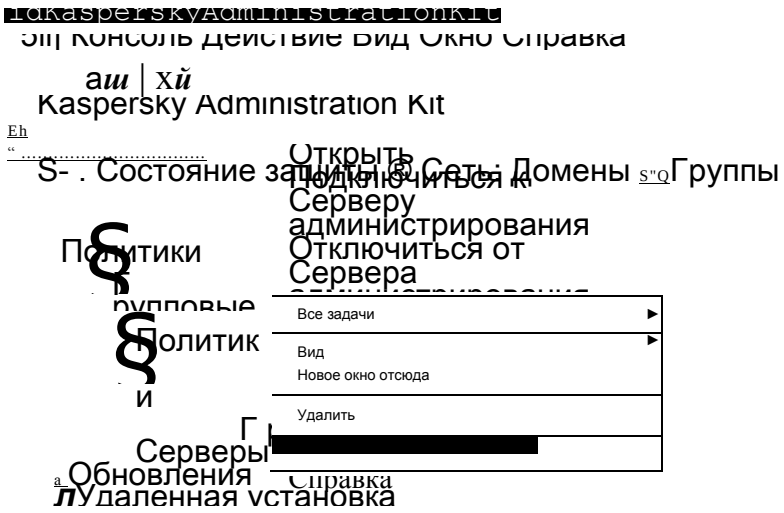


Рис. 5.83. Контекстное меню Сервера администрирования

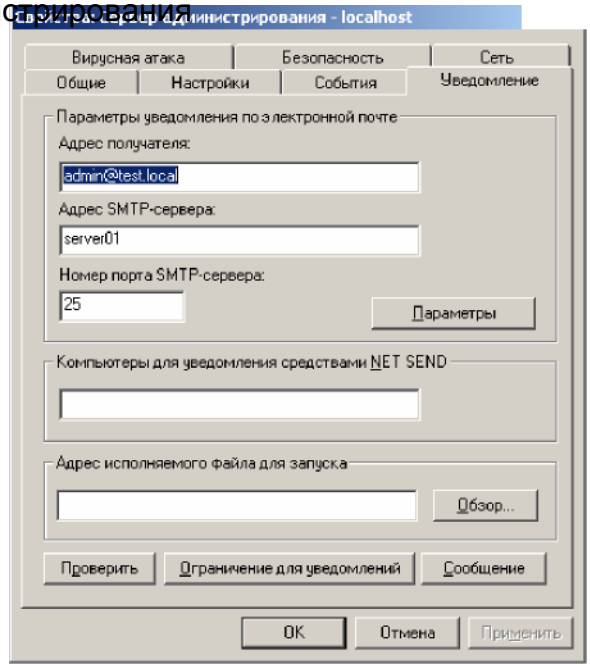


Рис. 5.84. Свойства Сервера администрирования Во-вторых, сам перечень событий для каждого антивирусного приложения задается в соответствующих политиках. Например, политика Антивируса Касперского для WindowsWorkstations(созданная Мастером первоначальной настройки (см. п. 5.3.5)), располагается в папке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

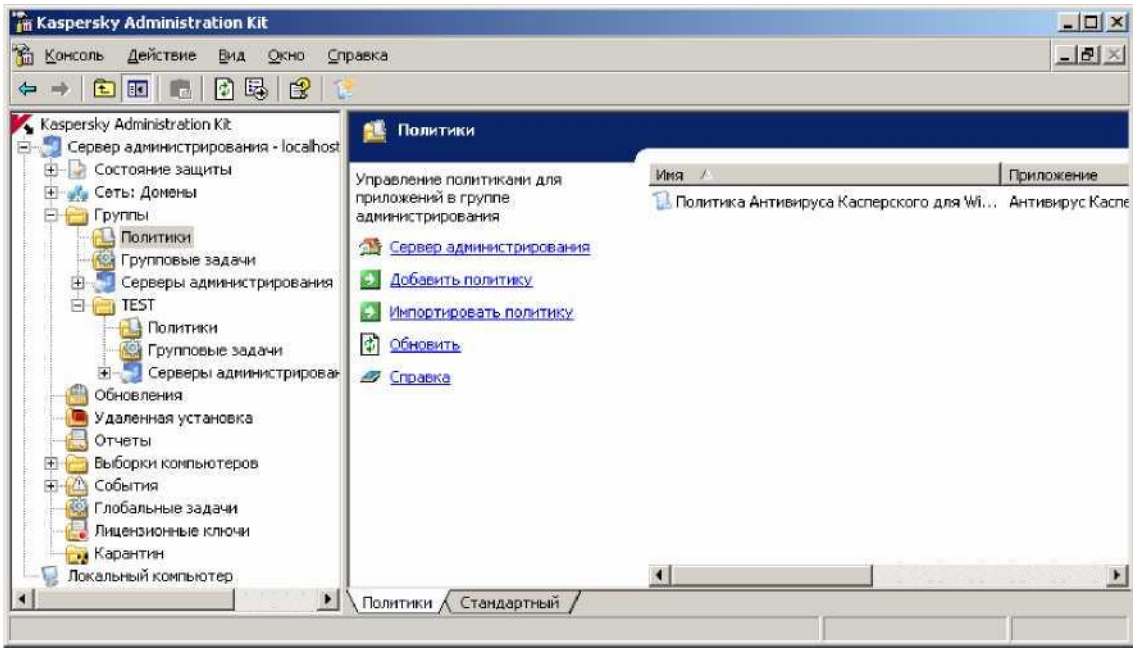


Рис. 5.85. Расположение глобальных политик Перечень событий и варианты реагирования располагаются в политике на закладке «События» (рис. 5.86). Выберите нужные Вам события для каждого уровня важности и включите параметр «Уведомлением по электронной почте». Если Вы хотите задать адрес электронной почты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

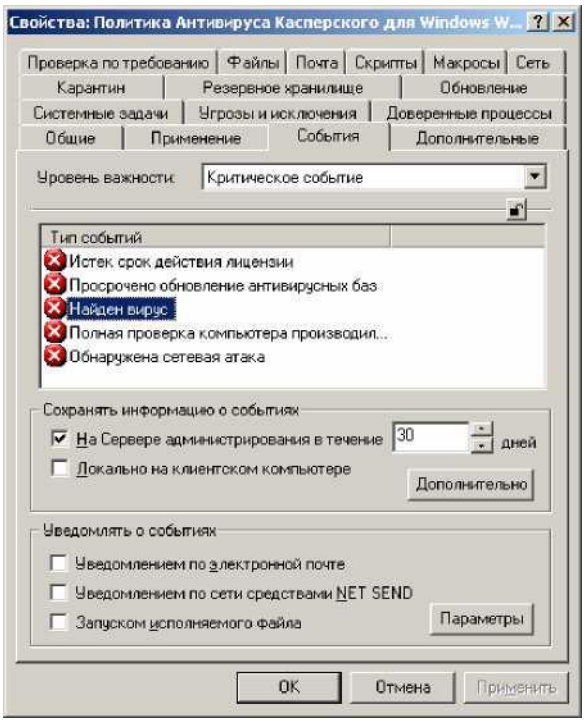


Рис. 5.86. Закладка События

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.

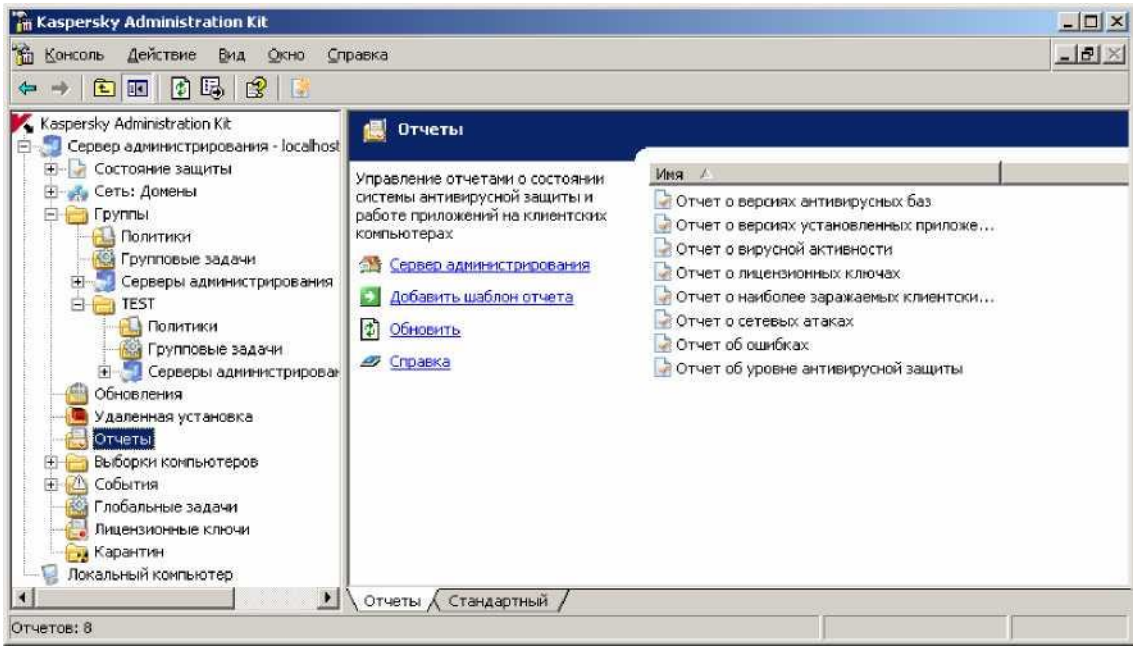


Рис. 5.87. Узел Отчеты

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.

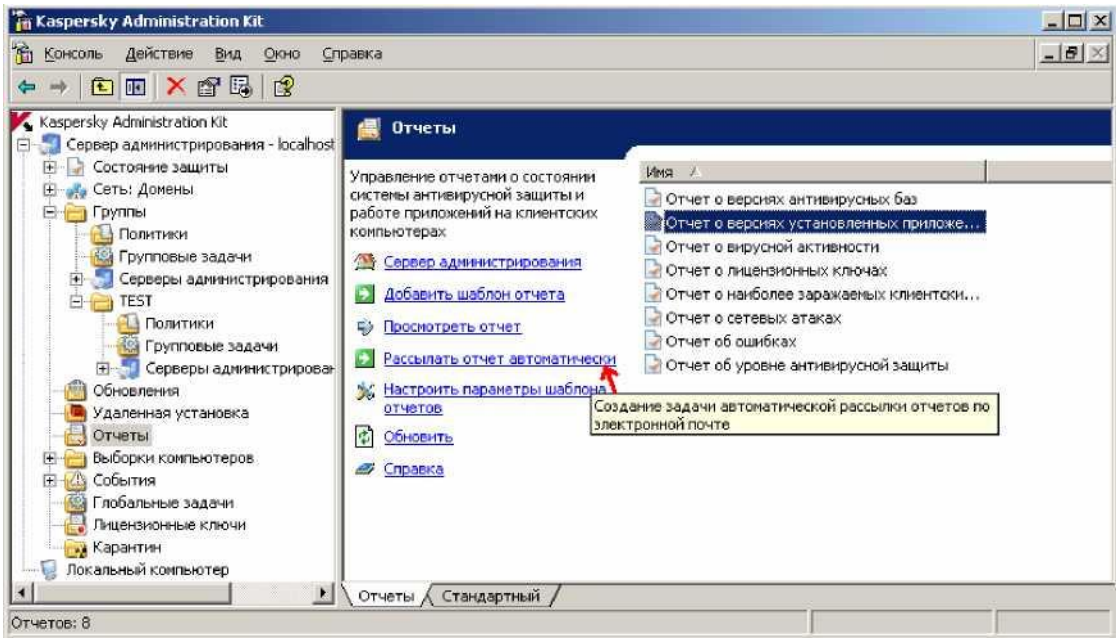


Рис. 5.89. Узел Отчеты

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).

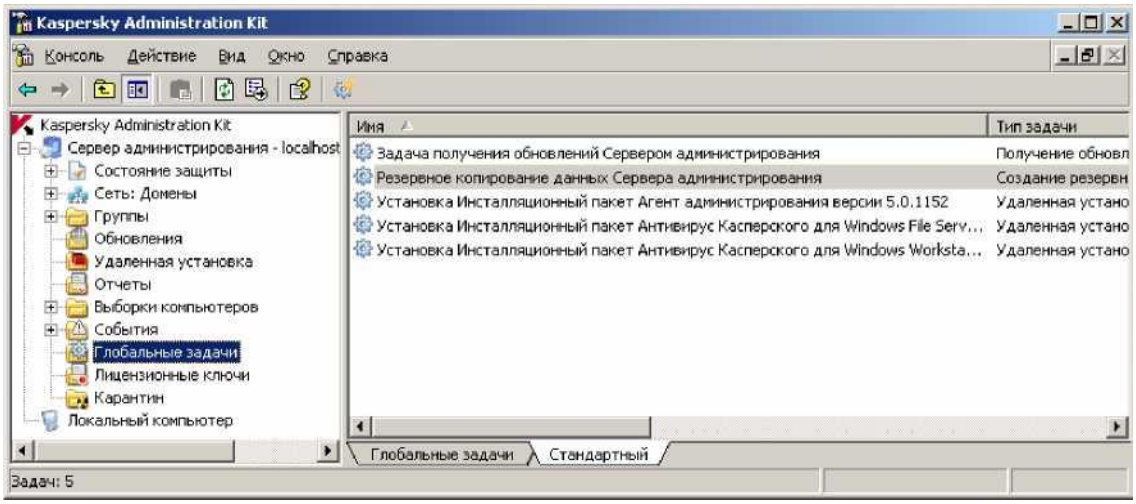


Рис. 5.90. Задача «Резервное копирование...»

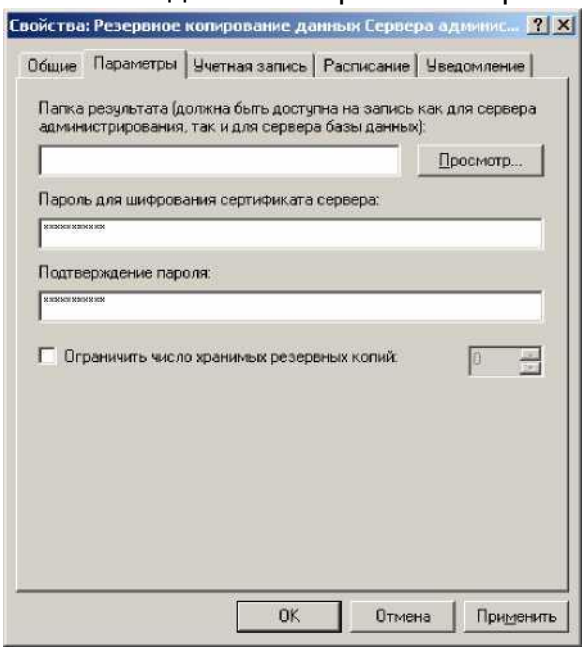


Рис. 5.91. Закладка «Параметры»

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.local`и `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.local`и `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 serverOIи clientOI. 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 - serverOI, 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):

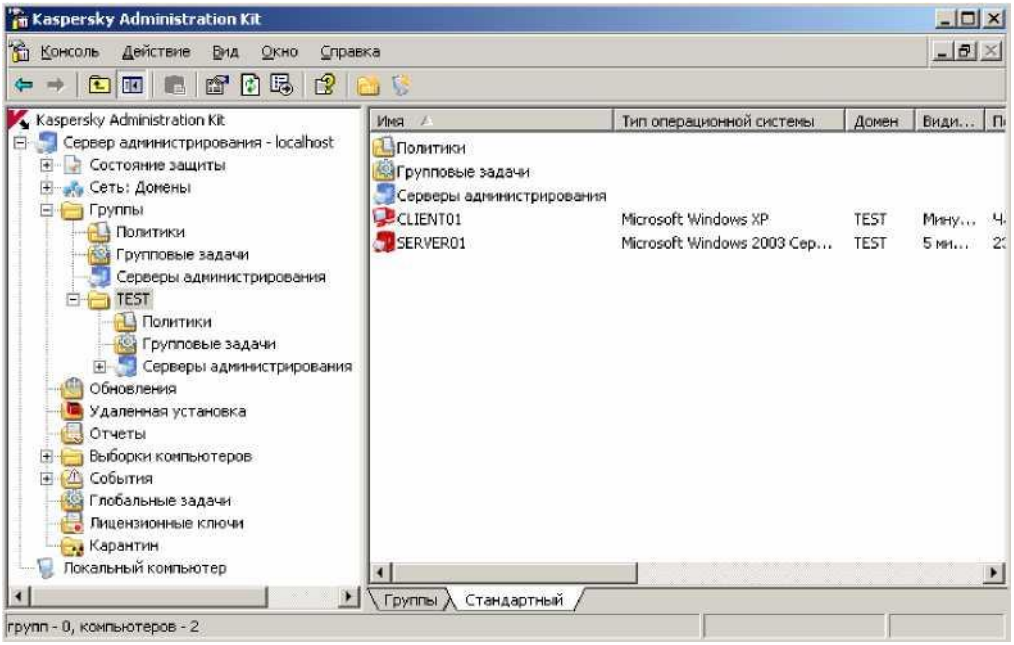


Рис. 5.92. Консоль администрирования

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):

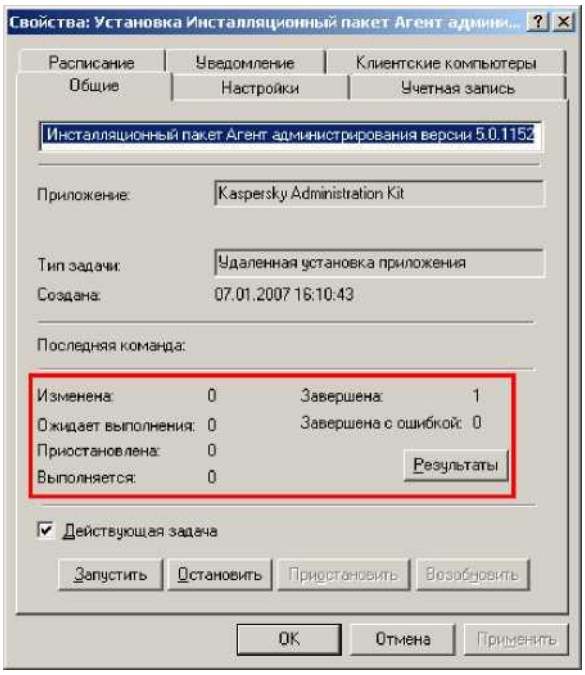


Рис. 5.93. Окно свойств задачи

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 WindowsWork- station») 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.

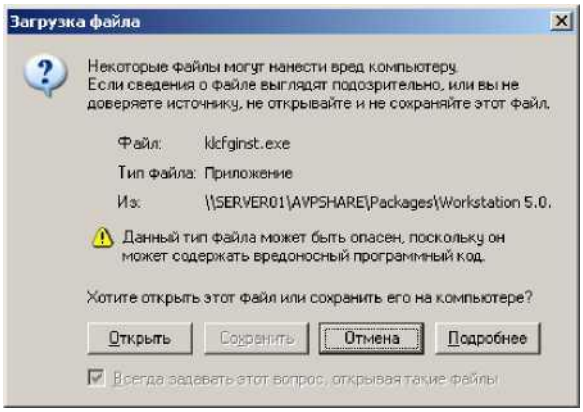


Рис. 5.94. Предупреждение ОС

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.

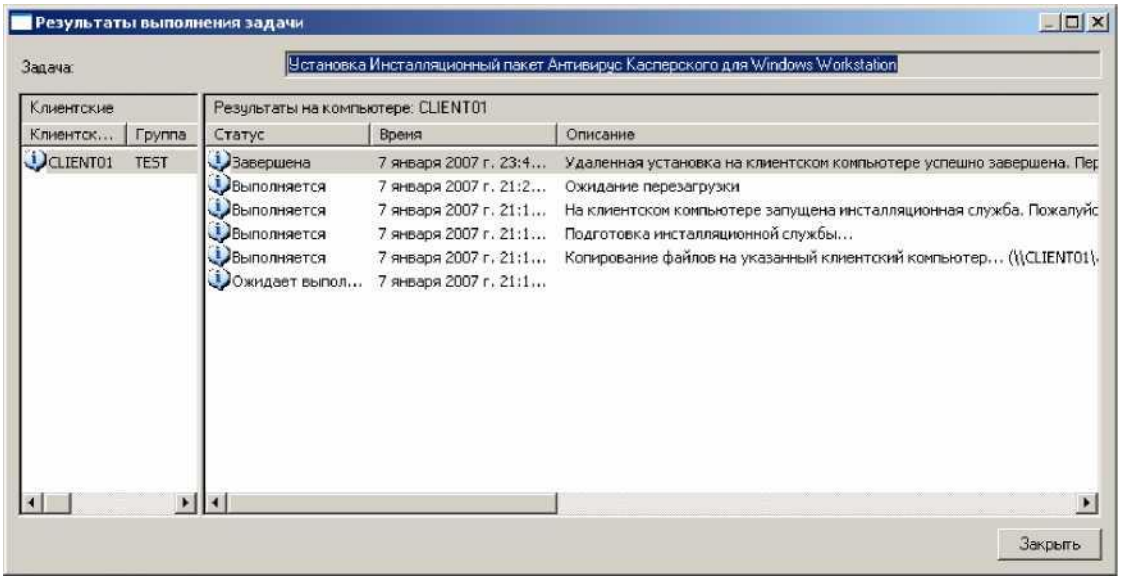


Рис. 5.95. Результаты успешного выполнения задачи

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.

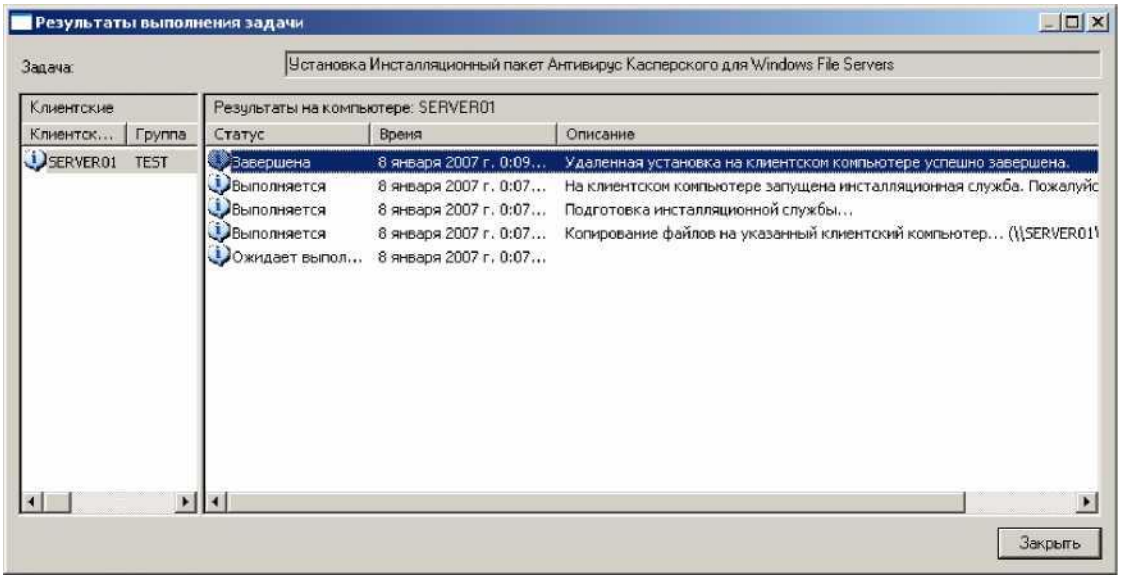


Рис. 5.96. Результаты выполнения задачи

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 cli- ent01.

17. Ещё раз проверьте дату создания антивирусных баз на компьютерах serverOIи clientOI(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 clientOIдля уведомления администратора по электронной почте.

1. Зарегистрируйтесь на компьютере serverOIпод 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 - serverOI, 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 clientOI.

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 serverOIпод 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 «ОК». Нажмите кнопку «ОК».
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«ОК». 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.

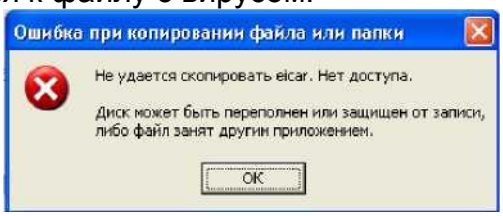


Рис. 5.97. Сообщение ОС

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 «ОК».

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

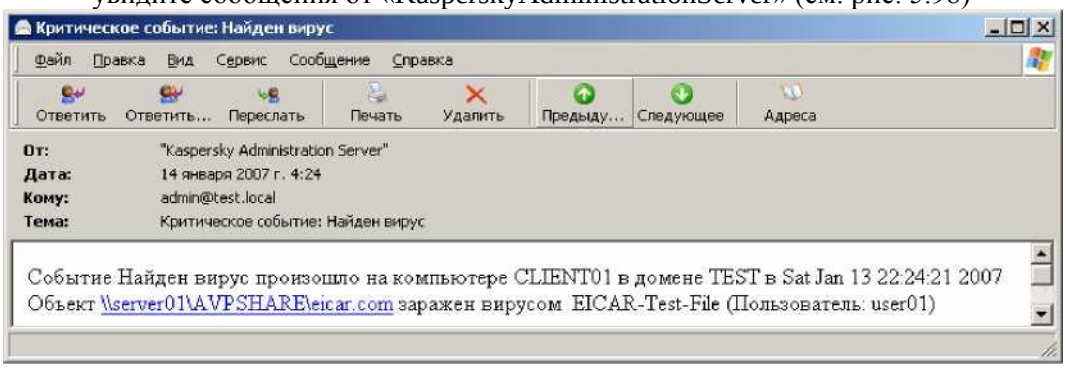


Рис. 5.98. Уведомление о событии

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.localc 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.

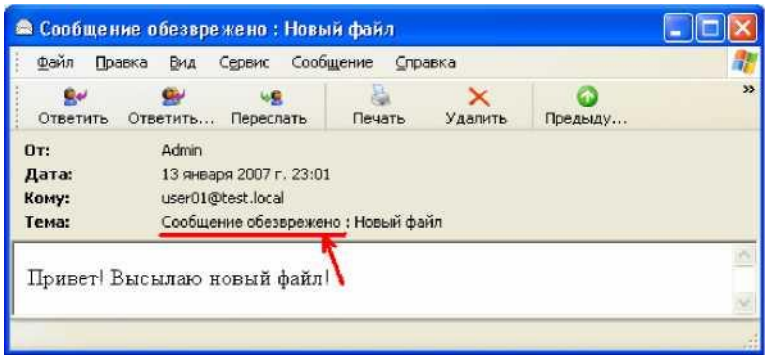


Рис. 5.99. Обезвреженное письмо

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.

ТЕМА: Центр обеспечения безопасности (Windows Security Center) в операционной системе Windows

СОДЕРЖАНИЕ

6. Центр обеспечения безопасности (Windows Security Center) в операционной системе Windows XP SP2

В этом занятии будет рассмотрен «Центр обеспечения безопасности Windows» (Windows Security Center) входящий в состав Windows XP SP2. Он разработан компанией Microsoft для автоматической проверки состояния трех основных компонентов ОС (брандмауэр, антивирус, система автоматического обновления). С помощью этого инструмента, пользователь имеет возможность не только контролировать состояние перечисленных выше компонентов, но и получать рекомендации по устранению возникающих с этими компонентами проблем [1].

кде всего

Для изучения материалов этого занятия необходим один компьютер под управлением операционной системы Windows XP Professional SP2 с настройками по умолчанию.

Для выполнения лабораторных работ необходимо два компьютера под управлением операционной системы Windows XP Professional SP2 с настройками по умолчанию.

6.1. Введение

Если ваш компьютер подключен к компьютерной сети (не важно, Интернет это или Интранет), то он уязвим для вирусов, атак злоумышленников и других вторжений. Для защиты компьютера от этих опасностей необходимо чтобы на нем постоянно работали межсетевой экран (брандмауэр), антивирусное ПО (с последними обновлениями) [2]. Кроме того, необходимо чтобы все последние обновления были также установлены на вашем компьютере.

Не каждый пользователь может постоянно следить за этим. Не каждый пользователь знает, как это осуществить. И даже если пользователь компетентен в этих вопросах, у него просто может не хватать времени на такие проверки. Компания Microsoft позаботилась обо всех этих пользователях, включив в состав SP2 для Windows XP такой инструмент. Он называется «Центр обеспечения безопасности Windows» (Windows Security Center) (рис. 6.1).

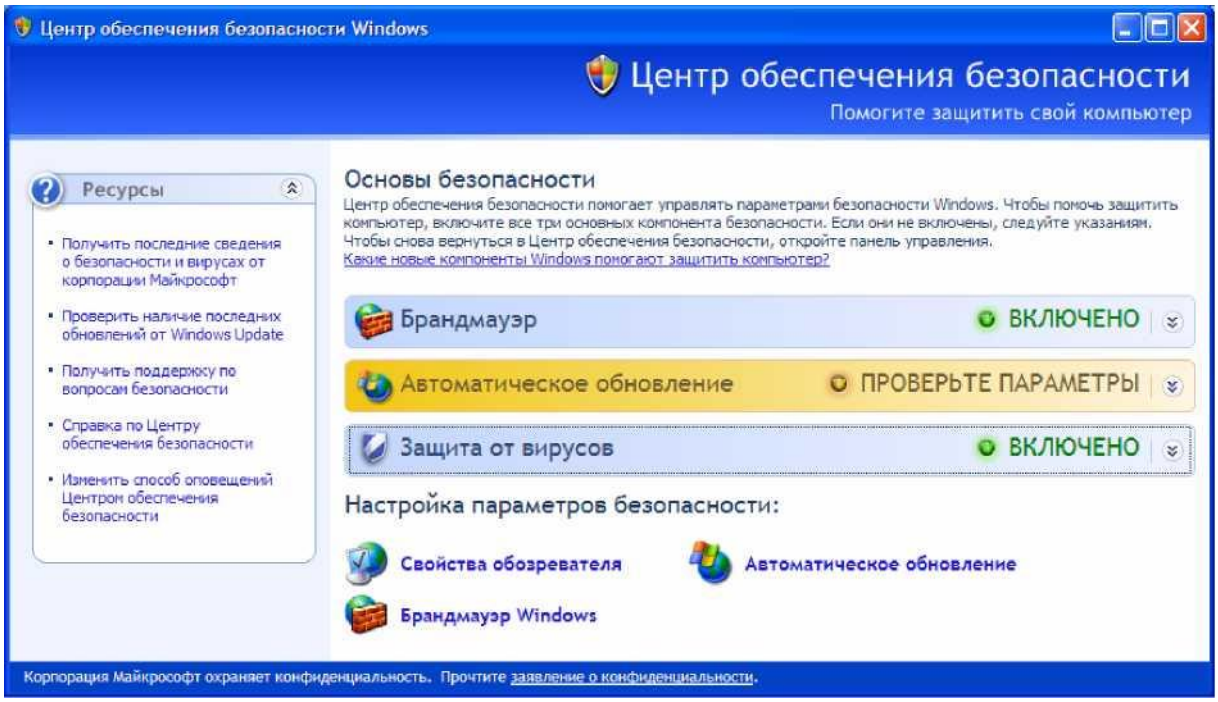


Рис. 6.1. Центр обеспечения безопасности Windows

Основное назначение этого инструмента - информировать и направлять пользователя в нужном направлении. Во-первых, он постоянно контролирует состояния трех основных компонентов ОС (брандмауэр, антивирус, система автоматического обновления). Если параметры любого из этих компонентов не будут удовлетворять требованиям безопасности компьютера, то пользователь получит соответствующее уведомление. Например, на рис. 6.2 представлено одно из таких уведомлений.

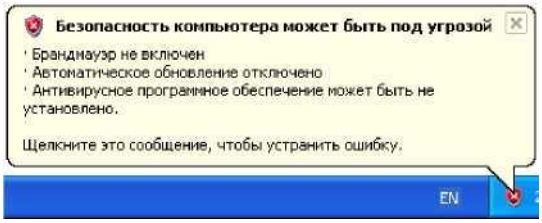


Рис. 6.2. Оповещение

Во-вторых, при открытии «Центра обеспечения безопасности Windows» пользователь может не только получить конкретные рекомендации о том, как исправить сложившуюся ситуацию, но также узнать, где находятся другие настройки связанные с безопасностью компьютера и где на сайте Microsoft можно прочитать дополнительную информацию по обеспечению безопасности компьютера.

Необходимо сразу отметить, что при подключении компьютера к домену, в «Центре обеспечения безопасности Windows» не отображаются сведения о состоянии безопасности компьютера (см. рис. 6.3) и не выполняется отправка сообщений безопасности. Считается, что в этом случае параметрами безопасности должен управлять администратор домена [3].

Для того чтобы включить «Центр для обеспечения безопасности Windows» для компьютера входящего в состав домена, необходимо в групповой политике домена включить параметр «Конфигурация компьютера, Административные шаблоны, Компоненты Windows, Центр обеспечения безопасности, Включить “Центр обеспечения безопасности” (только для компьютеров в домене)».

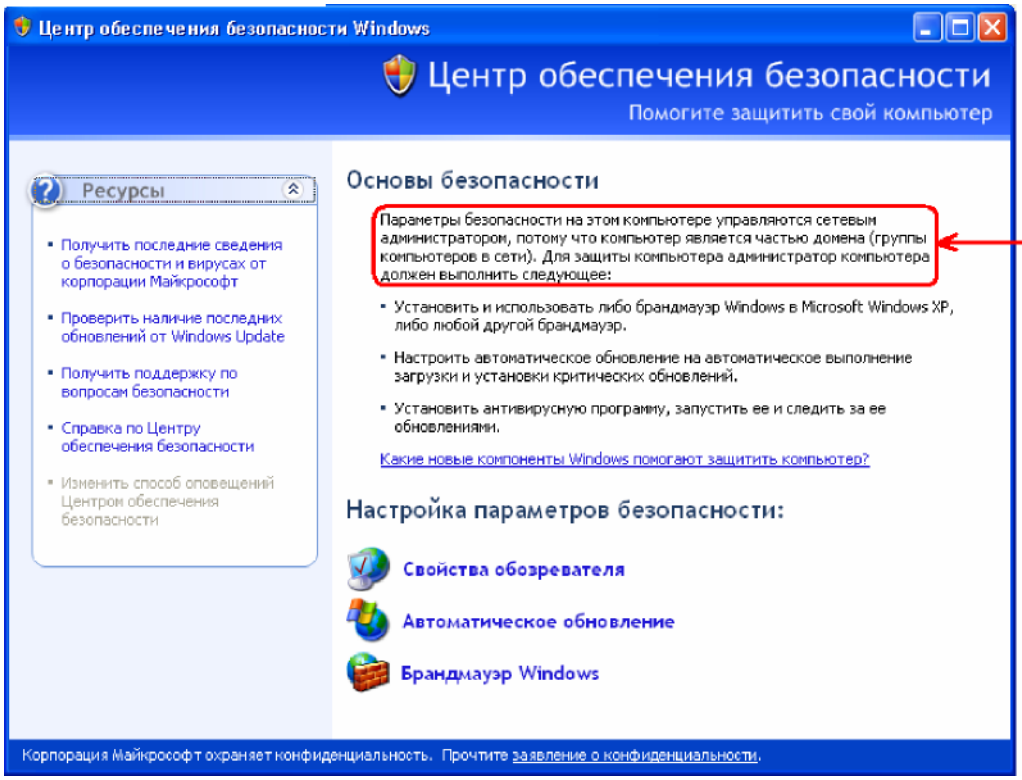


Рис. 6.3. Центр обеспечения безопасности Windows

6.2. Параметры безопасности Windows

Чтобы открыть «Центр обеспечения безопасности Windows», нажмите кнопку «Пуск», выберите команду «Панель управления», затем дважды щелкните значок «Центр обеспечения безопасности» (см. рис. 6.4).

Рис. 6.4. Значок

Окно Центра обеспечения безопасности Windows можно условно разделить на три части (см. рис. 6.5).

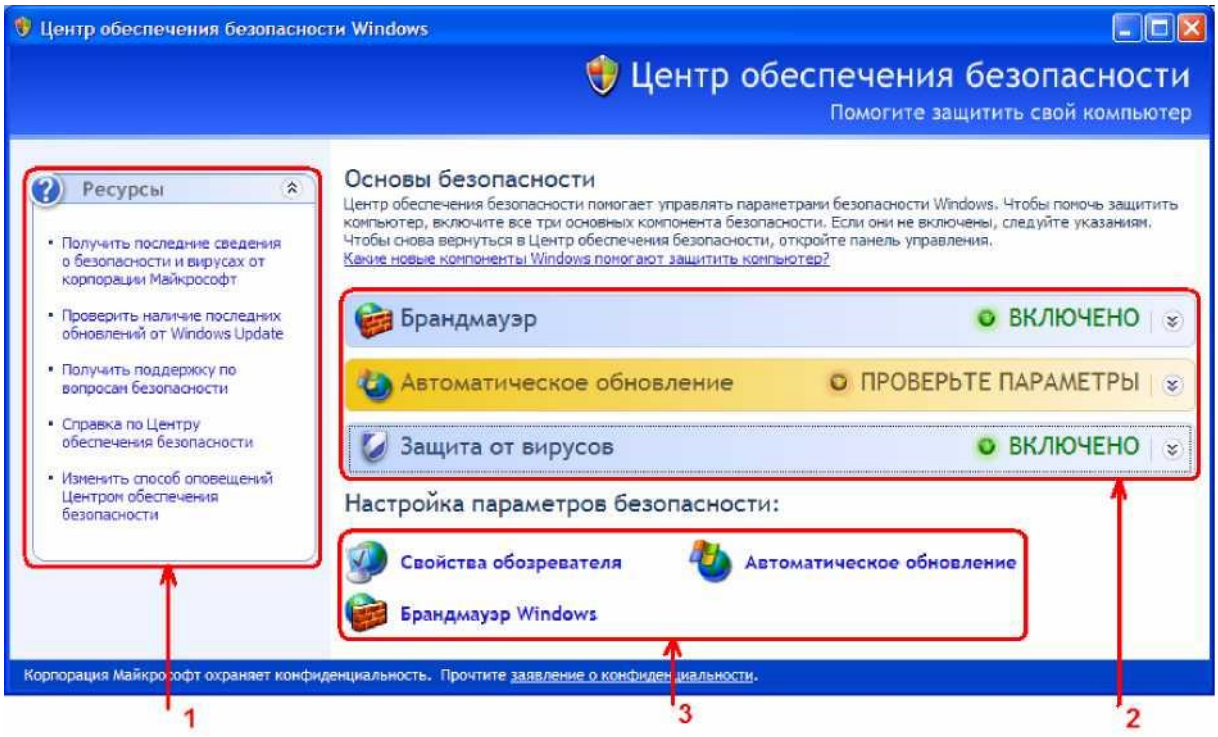


Рис. 6.5. Центр обеспечения безопасности

1. Ресурсы. Здесь располагаются ссылки для перехода к Интернетресурсам, к встроенной в Windows справочной службе и к окну настройки параметров оповещений.

2. Компоненты безопасности. Здесь располагаются информационные элементы трех основных компонентов безопасности: брандмауэр, автоматическое обновление, антивирусная защита.

3. Параметры безопасности. Здесь располагаются кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows.

Рассмотрим эти части более подробно.

6.2.1. Ресурсы

В разделе 1 первые три ссылки предназначены для перехода на соответствующие страницы на сайте Microsoft. Предпоследняя ссылка предназначена для открытия справочной службы Windows на странице «Общие сведения о центре обеспечения безопасности Windows». Последняя ссылка предназначена для открытия окна «Параметры оповещений» (см. рис. 6.6)

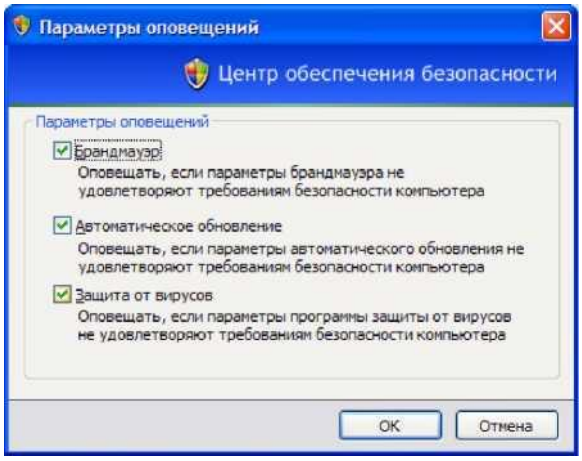


Рис. 6.6. Параметры оповещений

Если на компьютере установлен брандмауэр и антивирусное ПО не определяемое Центром обеспечения безопасности, вы можете отключить соответствующие оповещения (рис. 6.6)

6.2.2. Компоненты безопасности

В разделе 2 (см. рис. 6.5-2) каждое информационное табло информирует о состоянии соответствующего компонента. На рис. 6.7 представлены возможные состояния.

A	О ВКЛЮЧЕНО
B	О ПРОВЕРЬТЕ ПАРАМЕТРЫ
C	О ВЫКЛЮЧЕНО
D	© НЕ НАЙДЕНО
E	О СРОК ИСТЕК
F	О НЕ НАБЛЮДАЕТСЯ

Рис. 6.7. Состояния информационных табло

Состояния A-C понятны без комментариев. Состояние D - «Не найдено» соответствует невозможности определить присутствие соответствующего ПО (например, антивирус или брандмауэр). Состояние E - «Срок истек» возможно для антивирусной защиты когда обновления антивирусных баз устарели. Состояние F - «Не наблюдается» соответствует отключенному контролю над соответствующим компонентом.

Как указано в [1], «Центром обеспечения безопасности» применяется двухуровневый подход к определению состояния компонентов:

1. Проверка содержимого реестра и файлов со сведениями о состоянии ПО (Microsoft получает перечень файлов и параметров реестра от производителей ПО).

2. Сведения о состоянии ПО передаются от установленных программ средствами инструментария WMI (Windows Management Instrumentation - Инструментарий управления Windows).

На рис. 6.8 представлено одно из возможных состояний компонента «Брандмауэр». Нажав кнопку «Рекомендации...» вы получите возможность либо включить брандмауэр (рис. 6.9, кнопка «Включить сейчас»), либо отключить наблюдение за состоянием этого компонента (рис. 6.9, параметр «Я самостоятельно устанавливаю и слежу за брандмауэром»).

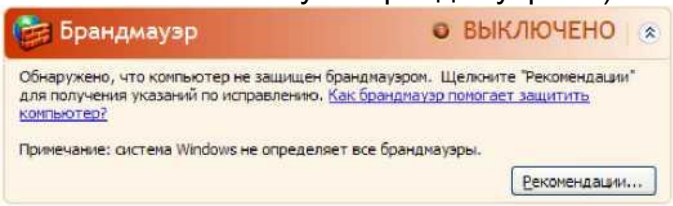


Рис. 6.8. Состояние «Брандмауэра»

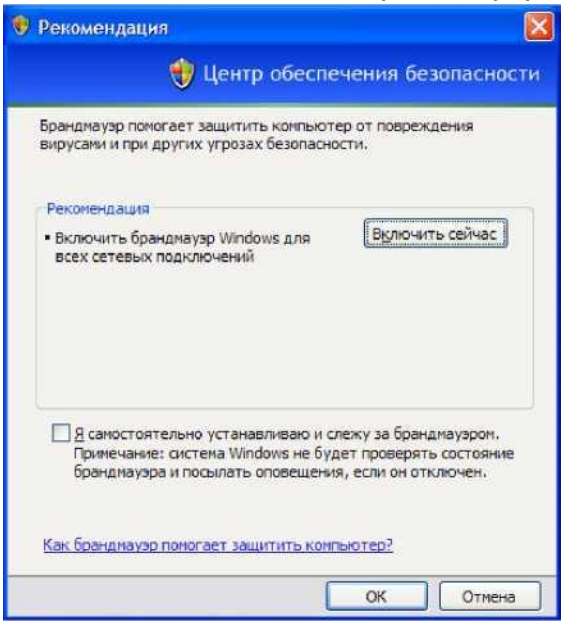


Рис. 6.9. Рекомендация

После нажатия кнопки «Включить сейчас» (см. рис. 6.9), если брандмауэр Windows будет успешно запущен, на экране появится соответствующее сообщение (см. рис. 6.10).

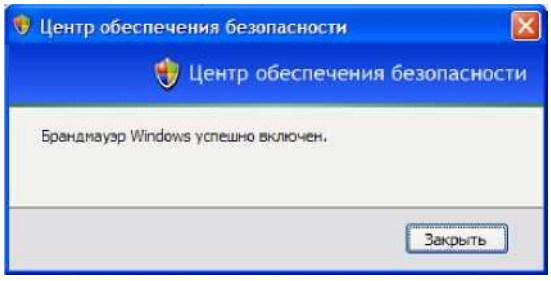


Рис. 6.10. Сообщение

На рис. 6.11 представлено одно из возможных состояний компонента «Автоматическое обновление». Нажав кнопку «Включить автоматическое обновление» вы включите рекомендуемый компанией Microsoft режим работы системы «Автоматическое обновление» (рис. 6.12). Подробнее о на-

стройках «Автоматического обновления» вы можете прочитать в разделе 6.4.

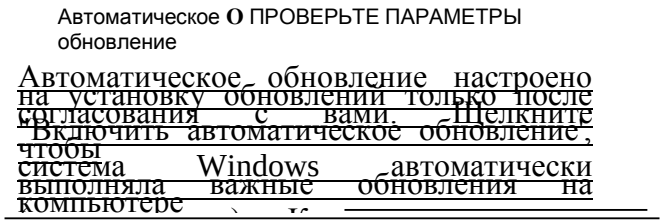


Рис. 6.11. Состояние «Автоматического обновления»

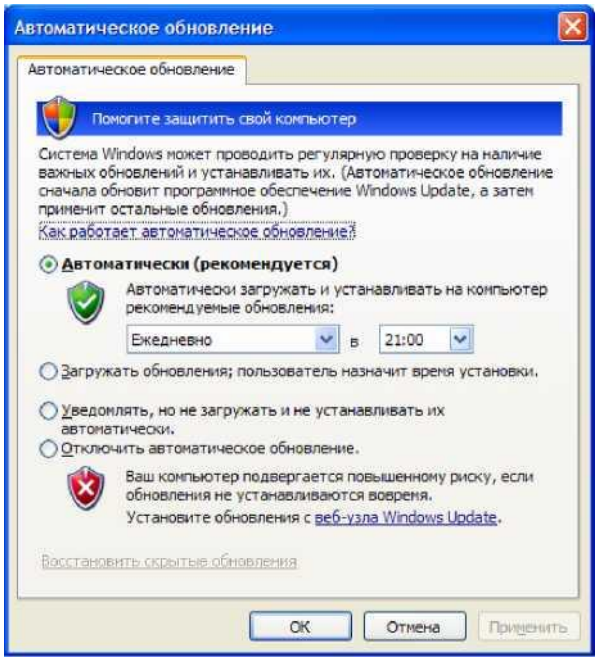


Рис. 6.12. Автоматическое обновление

Обратите внимание, что в зависимости от выставленного режима работы «Автоматического обновления» (см. рис. 6.12), в окне «Центра обеспечения безопасности» указывается краткое описание этого режима.

На рис. 6.13 представлено одно из возможных состояний компонента «Защита от вирусов». Нажав кнопку «Рекомендации...» вы получите лаконичные рекомендации (см. рис. 6.14): «включить антивирусную программу» (если она выключена), «установить другую антивирусную программу». В этом окне вы можете отключить наблюдение за состоянием этого компонента (параметр «Я самостоятельно устанавливаю и слежу за антивирусом»).

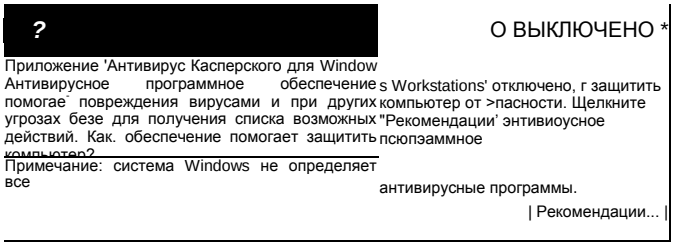


Рис. 6.13. Состояние «Защиты от вирусов»

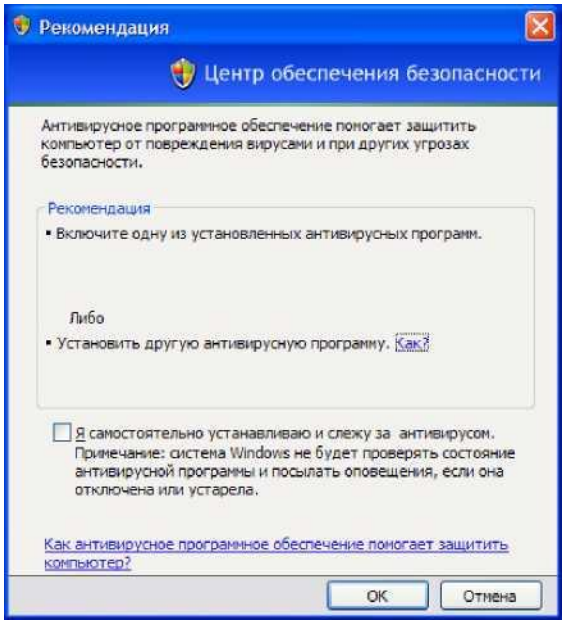


Рис. 6.14. Рекомендация

6.2.3. Параметры безопасности

Как уже было указано ранее, в разделе 3 (см. рис. 6.5-3) расположены кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows.

Нажав кнопку СЕОистЕаобозРевате,,я 5 вы попадете на закладку «Безопасность» в окне настроек обозревателя Internet Explorer (рис. 6.15). Подробнее об этих параметрах вы можете прочитать в разделе 6.3.

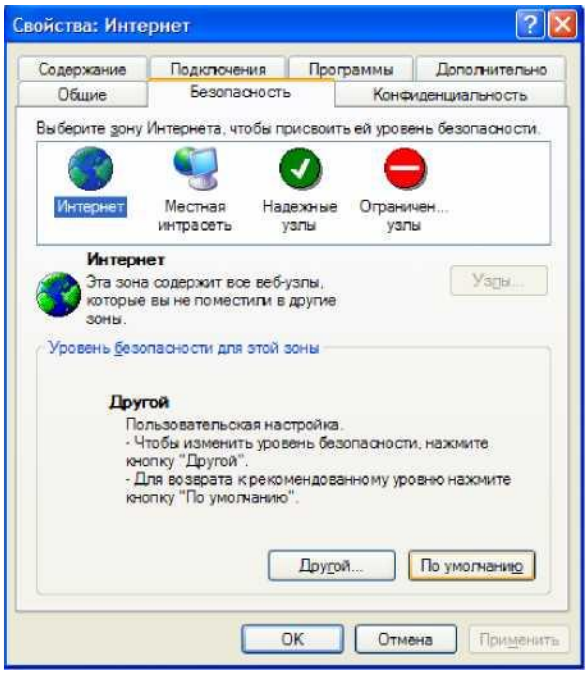


Рис. 6.15. Настройки Internet Explorer

Нажав кнопку Автоматическое обновлен^ вы 0ТКр0ете окно настроек «Автоматического обновления» (см. рис. 6.12). Подробнее о них вы можете прочитать в разделе 6.4.

Нажав кнопку Брандмауэр Wi,ldow5, вы попадете в соответствующее окно настроек (рис. 6.16). Подробнее об этих настройках вы можете прочитать в разделе 6.5.

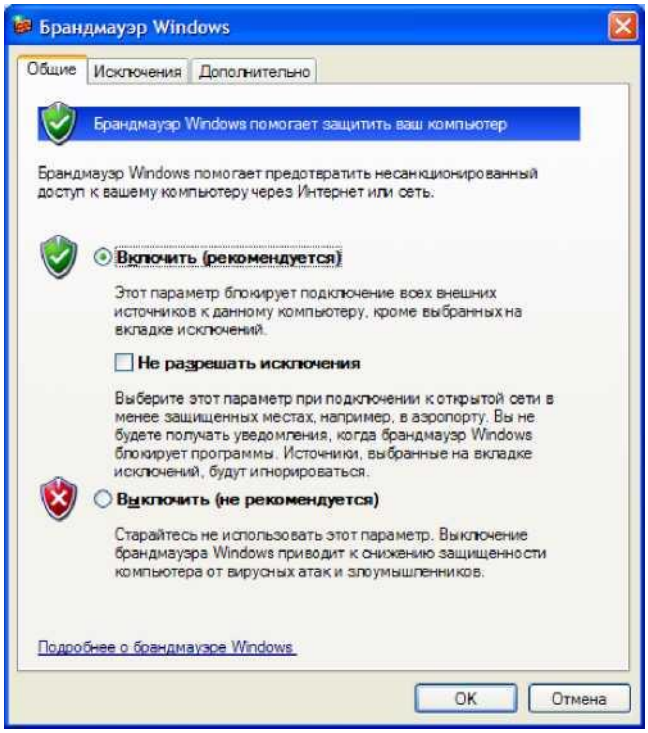


Рис. 6.16. Настройки Брандмауэра Windows В Windows XP SP2 для обозначения настроек касающихся безопасности (см. например, рис. 6.16), а также при оповещениях о состоянии безопасности компьютера (см. например, рис. 6.2) используются следующие значки[3]:

1. - Означает важные сведения и параметры безопасности.
2. *w* - Оповещает о потенциальном риске нарушения безопасности.
3. *'Ф* - Ситуация более безопасна. На компьютере используются рекомендуемые настройки безопасности.
4. *V* - Предупреждение: ситуация потенциально опасна. Измените настройки параметров безопасности, чтобы повысить безопасность компьютера.
5. Ф - Использовать текущие настройки параметров безопасности не рекомендуется.

6.3. Свойства обозревателя

Как уже указывалось ранее, нажав кнопку ^ СЕ0ИСТЕа обозревателя в <<ЦентРе обеспечения безопасности Windows», вы попадете в окно настроек обозревателя Internet Explorer на закладку «Безопасность» (рис. 6.17).

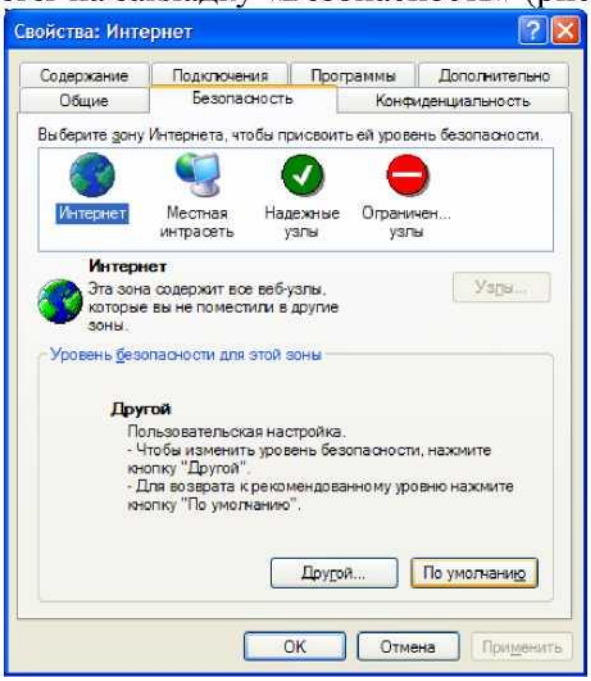


Рис. 6.17. Настройки безопасности Internet Explorer Рассмотрим параметры доступные на этой закладке. В верхней части расположены четыре зоны: Интернет, Местная интрасеть, Надежные узлы, Ограниченные узлы. В табл. 6.1 дано описание для каждой зоны.

Таблица 6.1

Описание зон

Зона	Какиеулы может содержать зона
Интернет	Содержит все веб-узлы, которые не помещены в другие зоны
Местная интрасеть	Может содержать указанные вами узлы. Может содержать все узлы интрасети, не перечисленные в других зонах, все узлы, подключаемые минуя прокси- сервер, все сетевые пути (UNC)
Надежные узлы	Может содержать указанные вами узлы.
Ограниченные узлы	Может содержать указанные вамиузлы.

Для всех зон, кроме зоны «Интернет», вы можете определить входящие в зону узлы. Для этого необходимо выбрать нужную зону (см. рис. 6.17) и нажать кнопку «Узлы...». Для зоны «Местная интрасеть» в этом случае откроется окно представленное на рис. 6.18. Если вы хотите указать конкретные узлы, нажмите кнопку «Дополнительно.». В результате появится окно представленной на рис. 6.19. Аналогичное окно будет открыто, если вы будете определять узлы, входящие в зоны «Надежные узлы» и «Ограниченные узлы». Только для зоны «Ограниченные узлы» будет отсутствовать параметр «Для всех узлов этой зоны требуется проверка серверов (https:)».

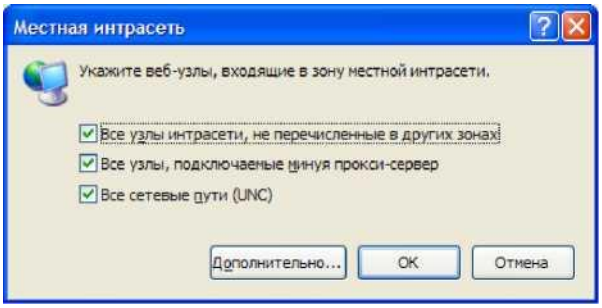


Рис. 6.18. Местная интрасеть

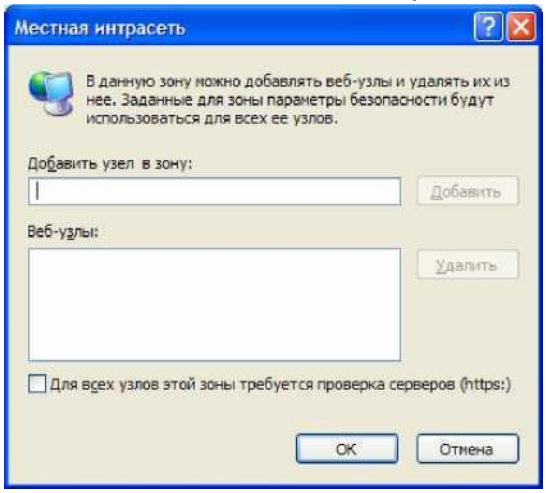


Рис. 6.19. Задание конкретных узлов

Каждой зоне можно присвоить нужный уровень безопасности: высокий, средний, ниже среднего, низкий. Низкий уровень безопасности соответствует минимальной защите и применяется для узлов, которым вы полностью доверяете.

Выберите нужную зону (см. рис. 6.17) и нажмите кнопку «По умолчанию». Закладка «безопасность» изменит свой вид (см. рис.6.20). В нижней части окна вы можете определить нужный уровень безопасности. Если вы не хотите использовать предлагаемые уровни безопасности, вы можете нажать кнопку «Другой...» и определить все параметры безопасности самостоятельно (см. рис. 6.21).

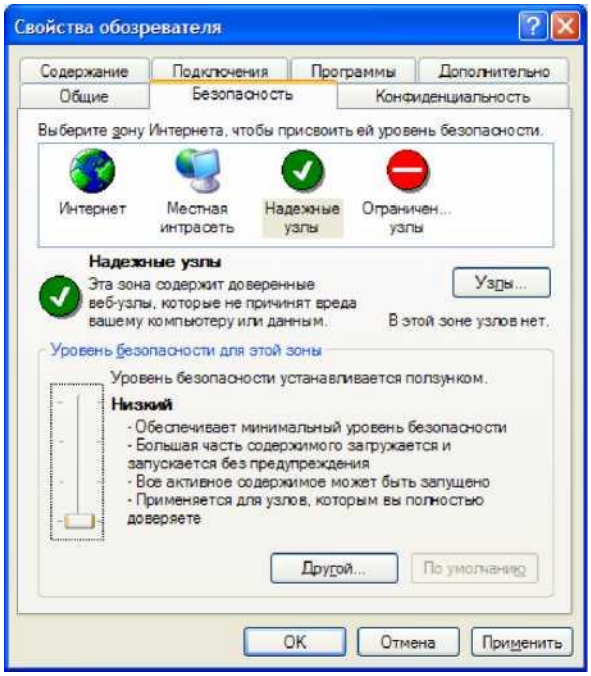


Рис. 6.20. Настройки безопасности Internet Explorer

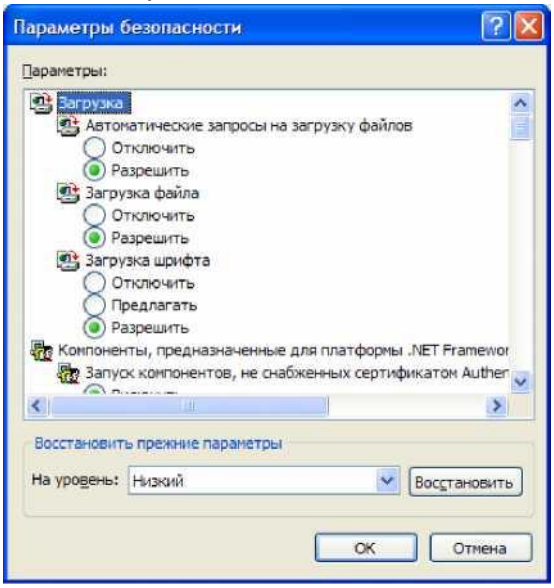


Рис. 6.21. Параметры безопасности

Описанные выше настройки безопасности обозревателя Internet Explorer также доступны для настройки через групповую политику (Конфигурация компьютера, Административные шаблоны, Компоненты Windows, Internet Explorer, Панель управления обозревателем, Страница безопасности).

6.4. Автоматическое обновление

Как уже указывалось ранее, нажав кнопку ^ в «Центре обеспечения безопасности Windows» вы откроете окно настроек «Автоматического обновления» (см. рис. 6.22).

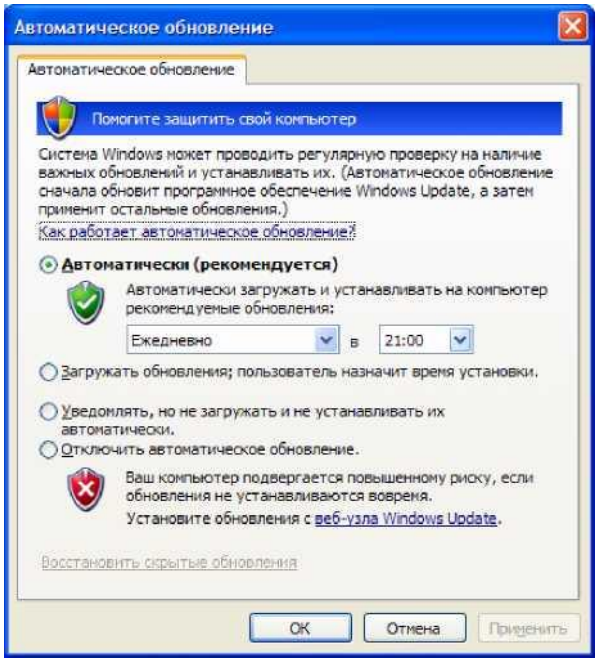


Рис. 6.22. Параметры автоматического обновления

Встроенная в Windows XP справочная система очень подробно описывает систему автоматического обновления. Для того чтобы воспользоваться этой справкой, щелкните по надписи «Как работает автоматическое обновление?» (см. рис. 6.22). Остановимся только на некоторых моментах.

Во-первых, необходимо различать понятия загрузка и установка обновлений. Загрузка означает процесс передачи файлов обновлений с сервера Microsoft (или с внутреннего сервера обновлений в организации) на компьютер пользователя. Установка обозначает собственно процесс инсталляции обновлений на компьютере пользователя. Возможна ситуация когда обновления загружены на пользовательский компьютер но еще не установлены.

Во-вторых, если вы выбрали вариант «Автоматически» (см. рис. 6.22), то обновления будут загружаться и устанавливаться в указанное вами время. Если компьютер в указанное время всегда выключен, то установка обновлений никогда не выполнится. При регистрации на компьютере пользователя с правами локального администратора, он может запустить установку вручную, не дожидаясь запланированного времени. При наступлении запланированного времени, пользователю будет выдано соответствующее предупреждение о начале установки обновлений. Если в этот момент в системе работает администратор, у него будет возможность отложить установку до следующего запланированного времени. У других пользователей (без прав администратора) возможности отменить запланированную установку обновлений не будет [4].

Во всех остальных случаях (кроме варианта «отключить автоматическое обновление»), уведомления о существующих обновлениях для вашего компьютера (готовых к загрузке или к установке) будут появляться только

при регистрации на вашем компьютере пользователя с правами локального администратора. Таким образом, если на компьютере вы постоянно работаете с учетной записью не входящей в группу локальных администраторов, то установка обновлений никогда не выполнится.

Описанные выше настройки автоматического обновления также доступны для настройки через групповую политику (Конфигурация компьютера, Административные шаблоны, Компоненты Windows, Windows Update). Кроме того, только через групповую политику можно задать дополнительные параметры. Например, можно указать адрес внутреннего сервера обновлений, который централизованно получает обновления с серверов Microsoft и отдает их внутренним компьютерам организации. В качестве примера такого сервера можно привести Microsoft® Windows Server™ Update Services (WSUS).

6.5. Брандмауэр Windows

Как уже указывалось ранее, нажав кнопку ® Брандмауэр Windows в «Центре обеспечения безопасности Windows» вы откроете окно настроек «Брандмауэра Windows» (см. рис. 6.23).

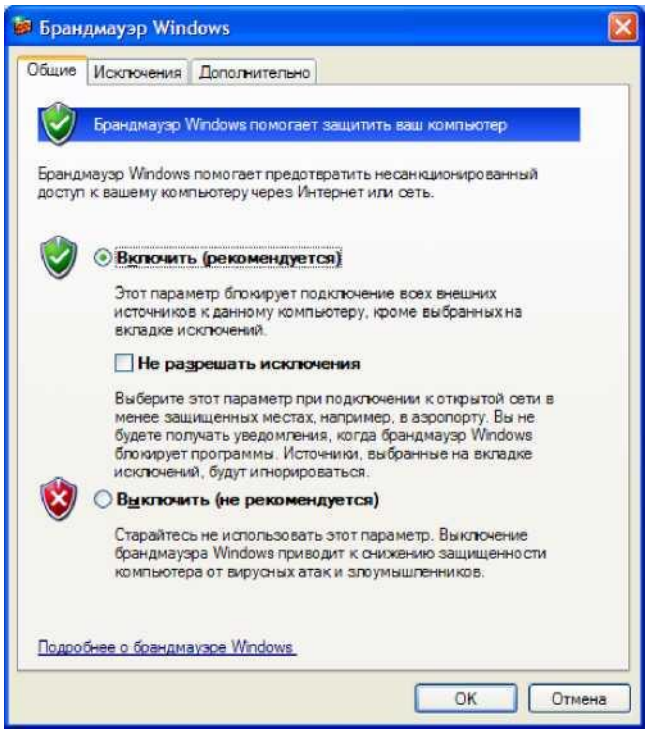


Рис. 6.23. Настройки Брандмауэра Windows Если вы щелкните по надписи «Подробнее о брандмауэре Windows» (см. рис. 6.23), то вы сможете прочитать краткую информацию о возможностях брандмауэра (межсетевого экрана) входящего в состав Windows XP SP2. Нет необходимости повторять эту информацию.

Отметим только, что в отличие от продуктов других производителей, встроенный брандмауэр Windows предназначен только для контроля вхо-

дящего трафика. Т.е. он защищает компьютер только от внешних вторжений. Он не контролирует исходящий трафик вашего компьютера. Таким образом, если на ваш компьютер уже установлен троянский конь или вирус, которые сами устанавливают соединения с другими компьютерами, брандмауэр Windows не будет блокировать их сетевую активность.

Кроме того, по умолчанию, брандмауэр защищает все сетевые соединения, и запрос входящего эха по протоколу ICMP запрещен. Это означает, что если на компьютере включен брандмауэр Windows, то проверять наличие такого компьютера в сети с помощью команды PING бессмысленное занятие.

Очень часто, в организациях, где используется программное обеспечение, требующее организации входящих соединений на пользовательские компьютеры, возникает необходимость открыть некоторые порты на компьютерах с установленной Windows XP SP2. Для решения этой задачи необходимо задать исключения в настройках брандмауэра Windows. Существует два способа решить эту задачу [5]:

1. Можно задать исключение, указав программу, требующую входящие соединения. В этом случае брандмауэр сам определит, какие порты необходимо открыть и откроет их только на время выполнения указанной программы (точнее, на время когда программа будет прослушивать этот порт).

2. Можно задать исключение, указав конкретный порт по которому программа ожидает входящие соединения. В этом случае порт будет открыт всегда. Даже когда эта программа не будет запущена. С точки зрения безопасности, этот вариант менее предпочтителен.

Существует несколько способов задать исключение в настройках брандмауэра Windows [6]. Можно воспользоваться графическим интерфейсом (см. рис. 6.24). Этот вариант достаточно подробно освещен в Центре справки и поддержки Windows XP SP2. Можно использовать доменную групповую политику. Этот вариант более предпочтителен при большом количестве компьютеров в организации. Рассмотрим его более подробно.

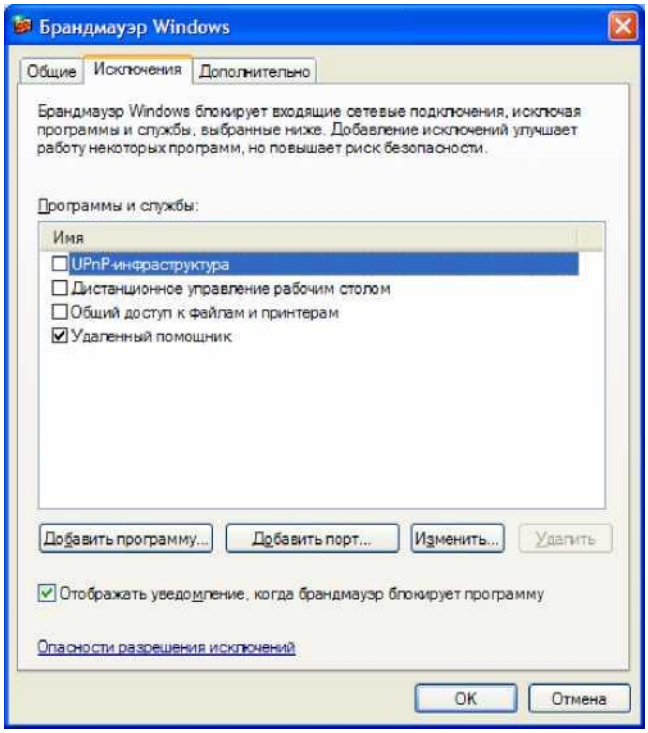


Рис. 6.24. Закладка Исключения

Параметры Брандмауэра Windows в групповой политике размещаются в узле «Конфигурация компьютера, Административные шаблоны, Сеть, Сетевые подключения, Брандмауэр Windows».

При настройке через групповую политику, вам необходимо настроить два профиля [6]:

1. Профиль домена. Настройки этого профиля используются, когда компьютер подключен к сети содержащей контроллер домена организации.

2. Стандартный профиль. Настройки этого профиля используются, когда компьютер не подключен к сети содержащей контроллер домена организации. Например, если ноутбук организации используется в командировке и подсоединен к Интернету через Интернет-провайдера. В этом случае настройка брандмауэра должны быть более строгими по сравнению с настройками доменного профиля, так как компьютер подключается к публичной сети, минуя межсетевые экраны своей организации.

Рассмотрим, как задать исключения для программы и для заданного порта. В качестве конкретного примера, рассмотрим, обращение Сервера администрирования Kaspersky Administration Kit к компьютеру на котором установлен Агент администрирования для получения информации о состоянии антивирусной защиты (подробнее см. занятие 5). В этом случае необходимо чтобы на клиентском компьютере был открыт порт UDP 15000 или разрешен прием входящих сообщений программой «C:\Program Files\Kaspersky Lab\NetworkAgent\klnagent.exe».

6.5.1. Создание исключения для программы

Настроим параметры групповой политик так, чтобы брандмауэр всегда работал, но пропускал входящие соединения для программы «C:\Program Files\Kaspersky Lab\NetworkAgent\klnagent.exe». Укажем также, что эта программа будет принимать входящие соединения только с адреса 192.168.0.1.

Для этого необходимо изменить параметры (см. табл. 6.2) расположенные в узле «Конфигурация компьютера, Административные шаблоны, Сеть, Сетевые подключения, Брандмауэр Windows, Профиль домена». Параметры не указанные в этой таблице могут иметь состояние «Не задана».

Таблица 6.2

Параметры групповой политики

Параметр	**Состояние**
Брандмауэр Windows: Защитить все сетевые подключения	**Включена**
Брандмауэр Windows: Не разрешать исключения	**Отключена**
Брандмауэр Windows: Задать исключения для программ	**Включена.** **%programfiles%\Kaspersky Lab\NetworkAgent\klnagent.exe:192.168.0.1:enabled:KasperskyAgent**

Формат задания исключения для программ следующий [6]:

*ProgramPath***:***Scope***:Enabled Disabled:** *ApplicationName*

где *ProgramPath* -путь к программе и имя файла,

Scope - один или несколько адресов разделенных запятыми (например, «*» - все сети (кавычки не указываются); 192.168.0.1 - один адрес; 192.168.10.0/24 - подсеть; «localsubnet» - локальная подсеть),

Enabled|Disabled - состояние исключения (включено или выключено),

ApplicationName - описание исключения (текстовая строка).

После применения этих параметров (см. табл. 6.2), окно настроек брандмауэра будет выглядеть так (см. рис. 6.25). Обратите внимание на надпись «Некоторые параметры управляются групповой политикой».

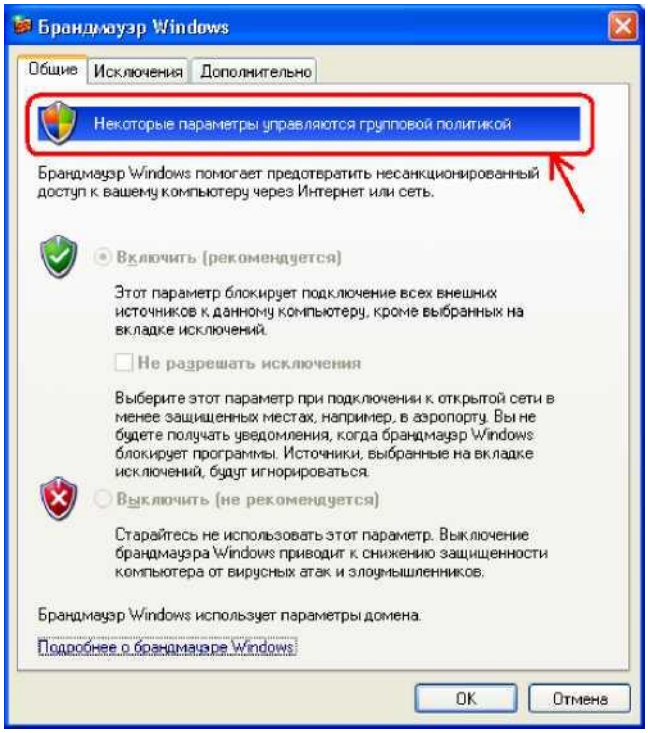


Рис. 6.25. Закладка Общие

Как видно на рисунке, настройки брандмауэра теперь закрыты для изменения локальным пользователям (в том числе с правами администратора). На рис. 6.26 представлена закладка Исключения на которой отмечено значение, добавленное групповой политикой домена.

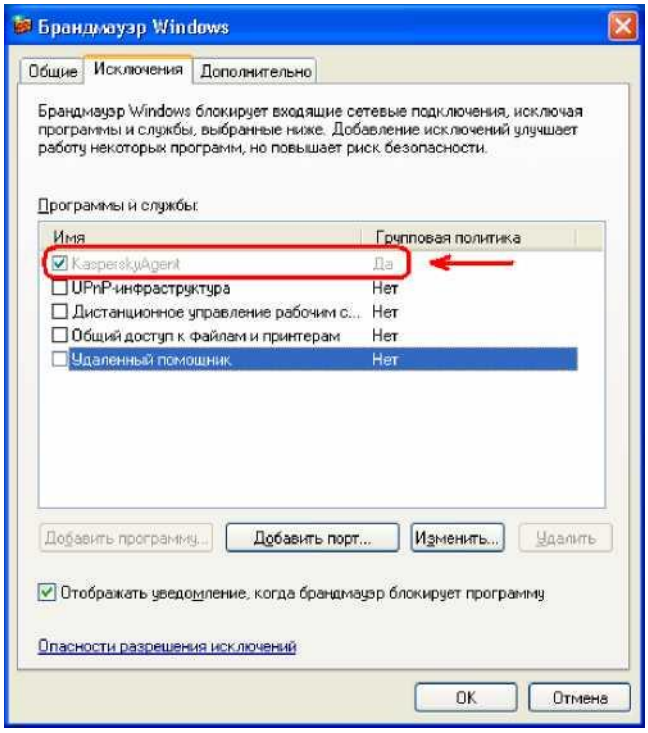


Рис. 6.26. Закладка Исключения

6.5.2. Создание исключения для порта

Настроим параметры групповой политик так, чтобы брандмауэр всегда работал, но пропускал входящие соединения с адреса 192.168.0.1 на порт UDP 15000.

Для этого необходимо изменить параметры (см. табл. 6.3) расположенные в узле «Конфигурация компьютера, Административные шаблоны, Сеть, Сетевые подключения, Брандмауэр Windows, Профиль домена». Параметры не указанные в этой таблице могут иметь состояние «Не задана».

Таблица 6.3

Параметры групповой политики

Параметр	**Состояние**
Брандмауэр Windows: Защитить все сетевые подключения	**Включена**
Брандмауэр Windows: Не разрешать исключения	**Отключена**
Брандмауэр Windows: Задать исключения для портов	**Включена.** **15000:UDP:192.168.0.1 :enabled:Kaspersky Agent Port**

Формат задания исключения для программ следующий [6]:

*Port#**:TCP*** UDP:Scope:Enabled Disabled:PortName

где *Port#* -номер открываемого порта,

TCP|UDP - тип порта,

Scope - один или несколько адресов разделенных запятыми (например, «*» - все сети (кавычки не указываются); 192.168.0.1 - один адрес; 192.168.10.0/24 - подсеть; «localsubnet» - локальная подсеть),

Enabled|Disabled - состояние исключения (включено или выключено),

PortName - описание исключения (текстовая строка).

6.6. Лабораторная работа. **Настройка брандмауэра**

В этой лабораторной работе Вы выполните настройку брандмауэра с помощью групповой политики и проверите его работу. В целях минимизации предварительных требований для выполнения работ будет использоваться групповая политика «Локальный компьютер». Компьютер client02 входит в рабочую группу (т.е. не введен в домен). Компьютер client01 может входить в рабочую группу или быть включенным в домен.

Предварительные требования

Для выполнения данной работы необходимо наличие двух (можно виртуальных) компьютеров под управлением Windows XP SP2 с настройками по умолчанию (в том числе - брандмауэр Windows включен). Один компьютер - client01 (IP=192.168.0.11/255.255.255.0). Второй компьютер - cli- ent02 (IP=192.168.0.12/255.255.255.0). Учетная запись администратора на обоих компьютерах - «Administrator», пароль «P@ssw0rd».

Лабораторная работа 1 выполняется на компьютерах clientOl (установка тестовых подключений с компьютером client02) и client02 (настройка брандмауэра, службы Telnet).

6.6.1. Упражнение 1. Проверка межсетевого взаимодействия

Вы проверите прохождение пакетов ICMP между компьютерами до, и после отключения брандмауэра.

1. Зарегистрируйтесь на компьютере clientOl под учетной записью Administrator с паролем P@ssw0rd.
2. Откройте командную строку. Для этого выполните команду «Пуск | Выполнить», введите **`cmd`** и нажмите OK.
3. Выполните команду **`ping 192.168.0.12`**. Статистика обмена пакетами должна сообщить о 100% потере пакетов. Почему?
4. Зарегистрируйтесь на компьютере client02 под учетной записью Administrator с паролем P@ssw0rd.
5. Выключите брандмауэр. Для этого выполните «Пуск | Панель управления | Центр обеспечения безопасности | Брандмауэр Windows». В окне настроек брандмауэра выберите вариант «Выключить» и нажмите OK. Вы сразу увидите уведомление Центра обеспечения безопасности «Безопасность компьютера может быть под угрозой. Брандмауэр не включен».
6. Переключитесь на компьютер client01. Вернитесь в окно с командной строкой.
7. Выполните команду **`ping 192.168.0.12`**. Статистика обмена пакетами должна сообщить об отсутствии потерь пакетов. Почему?

6.6.2. Упражнение 2. Включение службы Telnet

Вы включите службу Telnet на компьютере client02, создадите учетную запись для подключения к ней. Проверите подключение к службе Telnet с компьютера client01.

1. Зарегистрируйтесь на компьютере client02 под учетной записью Administrator с паролем P@ssw0rd.
2. Создайте учетную запись user3 с паролем P@ssw0rd. Для этого выполните команду «Пуск | Выполнить», введите **`compmgmt.msc`** , нажмите OK. Разверните узел «Локальные пользователи и группы». Откройте контекстное меню элемента «Пользователи» и выполните команду «Новый пользователь...». В поле «Пользователь:» введите **`user3`**. Укажите пароль «P@ssw0rd». Отключите параметр «Потребовать смену пароля при следующем входе в систему» и нажмите кнопку «Создать».
3. Создайте группу **`TelnetClients`** и добавьте в эту группу учетную запись **`user3`**. Для этого откройте контекстное меню элемента «Группы» и выполните команду «Создать группу.». В поле «Имя группы:» введите **`TelnetClients`**. Нажмите кнопку «Добавить». В появившем

ся окне в поле «Введите имена выбираемых объектов» введите user3 и нажмите кнопку «OK». Нажмите кнопку «Создать».

4. Изменим тип запуска службы Telnet с «Отключено» на «Вручную» и запустим её. Для этого выполните команду «Пуск | Выполнить», введите **`services.msc`**, нажмите OK. В правой части окна найдите службу Telnet и дважды щелкните по ней левой кнопкой мыши. В появившемся окне выберите Тип запуска «Вручную». Нажмите кнопку «Применить». Нажмите кнопку «Пуск». Запомните значение параметра «Исполняемый файл» (**`C:\WINDOWS\system32\tlntsvr.exe`**). Это значение нам понадобится при настройке исключения в брандмауэре. Нажмите кнопку «OK».
5. Переключитесь на компьютер client01. Вернитесь в окно с командной строкой.
6. Выполните команду **`telnet 192.168.0.12`**. Должно появиться приветствие программы-клиента Microsoft Telnet. На вопрос «Вы намерены передать информацию ..... Послать в любом случае (y/n):» введите **`n`** и нажмите «Enter». На запрос «login:» введите **`user3`**. На запрос «password:» введите P@ssw0rd. После появления сообщения «Вас приветствует Telnet-сервер...» введите команду **`exit`**. Нам удалось подключиться к Telnet-серверу.
7. Переключитесь на компьютер client02.
8. Включите брандмауэр. Для этого выполните «Пуск | Панель управления | Центр обеспечения безопасности | Брандмауэр Windows». В окне настроек брандмауэра выберите вариант «Включить» и нажмите OK.
9. Выполните команду **`telnet 192.168.0.12`**. Должно появиться сообщение: «Подключение к 192.168.0.12.Не удалось открыть подключение к этому узлу, на порт 23: Сбой подключения». Почему?

6.6.3. Упражнение 3. Настройка исключения для порта

На компьютере client02, с помощью групповой политики «Локальный компьютер», вы настроите исключение для порта TCP 23 (разрешим входящие подключения на этот порт из локальной подсети) и проверите подключение к службе Telnet с компьютера client01.

1. Зарегистрируйтесь на компьютере client02 под учетной записью Administrator с паролем P@ssw0rd.
2. Откройте редактор групповой политики «Локальный компьютер». Для этого выполните команду «Пуск | Выполнить», введите **`gpedit.msc`** , нажмите OK.
3. Откройте узел «Конфигурация компьютера, Административные шаблоны, Сеть, Сетевые подключения, Брандмауэр Windows, Стандартный профиль».

4. Включите параметр «Брандмауэр Windows: Защитить все сетевые подключения». Для этого дважды щелкните левой кнопкой мыши по этому параметру. В открывшемся окне выберите вариант «Включен» и нажмите кнопку «OK».
5. Отключите параметр «Брандмауэр Windows: Не разрешать исключения». Для этого дважды щелкните левой кнопкой мыши по этому параметру. В открывшемся окне выберите вариант «Отключен» и нажмите кнопку «OK».
6. Включите параметр «Брандмауэр Windows: Задать исключения для портов». Для этого дважды щелкните левой кнопкой мыши по этому параметру. В открывшемся окне выберите вариант «Включен» и нажмите кнопку «Показать...». Нажмите кнопку «Добавить...». В появившемся окне введите строку «23:TCP:localsubnet:enabled:Telnet Port». Нажмите кнопку «OK». Нажмите кнопку «OK».
7. Применим групповую политику. Для этого выполните команду «Пуск | Выполнить», введите gpupdate , нажмите OK.
8. Просмотрите параметры брандмауэра. Для этого выполните «Пуск | Панель управления | Центр обеспечения безопасности | Брандмауэр Win- dows». В окне настроек брандмауэра на закладке «Общие» должно быть отображено «Некоторые параметры управляются групповой политикой» и все параметры должны быть заблокированы для изменения. На закладке «Исключения» должно появиться исключение «Telnet Port».
9. Откройте командную строку. Для этого выполните команду «Пуск | Выполнить», введите cmd и нажмите OK.
10. Проверим состояние службы Telnet и порт, который эта служба прослушивает. Для этого выполните команду tlntadmn. На экран будут выведены параметры службы Telnet. Обратите внимание на параметр «Порт Telnet» и «Состояние». Они должны быть равны 23 и Stopped соответственно.

    11.Запустим службу Telnet. Для этого выполните команду tlntadmn start. В случае успешного запуска на экран будет выведено «The service was started successfully».
12. Переключитесь на компьютер client01. Вернитесь в окно с командной строкой.
13. Выполните команду telnet 192.168.0.12. Должно появиться приветствие программы-клиента Microsoft Telnet. На вопрос «Вы намерены передать информацию ..... Послать в любом случае (y/n):» введите n и нажмите «Enter». На запрос «login:» введите user3. На запрос «password:» введите P@ssw0rd. После появления сообщения «Вас приветствует Telnet-сервер.» введите команду exit. Нам удалось подключиться к Telnet-серверу.

6.6.4. Упражнение 4. Настройка исключения для программы

Как вы видели в упражнении 2, службе Telnet соответствует исполняемый файл «C:\WINDOWS\system32\tlntsvr.exe».

На компьютере client02, с помощью групповой политики «Локальный компьютер», вы настроите исключение для этого исполняемого файла (разрешим входящие подключения для этой программы из локальной подсети) и проверите подключение к службе Telnet с компьютера clientOl. После этого, вы измените номер порта для службы Telnet на 1000 и проверите, что подключение к службе Telnet всё ещё возможно (брандмауэр сам определяет порт, по которому работает указанный исполняемый файл и разрешает открытые им входящие подключения).

1. Зарегистрируйтесь на компьютере client02 под учетной записью Administrator с паролем P@ssw0rd.
2. Откройте редактор групповой политики «Локальный компьютер». Для этого выполните команду «Пуск | Выполнить», введите gpedit.msc , нажмите OK.
3. Откройте узел «Конфигурация компьютера, Административные шаблоны, Сеть, Сетевые подключения, Брандмауэр Windows, Стандартный профиль».
4. Включите параметр «Брандмауэр Windows: Защитить все сетевые подключения». Для этого дважды щелкните левой кнопкой мыши по этому параметру. В открывшемся окне выберите вариант «Включен» и нажмите кнопку «OK».
5. Отключите параметр «Брандмауэр Windows: Не разрешать исключения». Для этого дважды щелкните левой кнопкой мыши по этому параметру. В открывшемся окне выберите вариант «Отключен» и нажмите кнопку «OK».
6. Отключите параметр «Брандмауэр Windows: Задать исключения для портов». Для этого дважды щелкните левой кнопкой мыши по этому параметру. В открывшемся окне выберите вариант «Отключен» и нажмите кнопку «OK».
7. Включите параметр «Брандмауэр Windows: Задать исключения для программ». Для этого дважды щелкните левой кнопкой мыши по этому параметру. В открывшемся окне выберите вариант «Включен» и нажмите кнопку «Показать...». Нажмите кнопку «Добавить...». В появившемся окне введите строку «%windir%\system32\tlntsvr.exe:localsubnet:enabled: Telnet server». Нажмите кнопку «OK». Нажмите кнопку «OK».
8. Применим групповую политику. Для этого выполните команду «Пуск | Выполнить», введите gpupdate , нажмите OK.
9. Просмотрите параметры брандмауэра. Для этого выполните «Пуск | Панель управления | Центр обеспечения безопасности | Брандмауэр Win- dows». В окне настроек брандмауэра на закладке «Общие» должно быть отображено «Некоторые параметры управляются групповой полити-

кой» и все параметры должны быть заблокированы для изменения. На закладке «Исключения» должно появиться исключение «Telnet Server».

10.Откройте командную строку. Для этого выполните команду «Пуск | Выполнить», введите cmd и нажмите OK.

11. Проверим состояние службы Telnet и порт, который эта служба прослушивает. Для этого выполните команду tlntadmn. На экран будут выведены параметры службы Telnet. Обратите внимание на параметр «Порт Telnet». Он должен быть равен 23.
12. Если параметр «Состояние» равен «Stopped», то запустите службу Telnet. Для этого выполните команду tlntadmn start. В случае успешного запуска на экран будет выведено «The service was started successfully».
13. Переключитесь на компьютер client01. Вернитесь в окно с командной строкой.
14. Выполните команду telnet 192.168.0.12. Должно появиться приветствие программы-клиента Microsoft Telnet. На вопрос «Вы намерены передать информацию ..... Послать в любом случае (y/n):» введите n и нажмите «Enter». На запрос «login:» введите user3. На запрос «password:» введите P@ssw0rd. После появления сообщения «Вас приветствует Telnet-сервер...» введите команду exit. Нам удалось подключиться к Telnet-серверу.
15. Переключитесь на компьютер client02. Вернитесь в окно с командной строкой.
16. Изменим порт для службы Telnet на значение 1000. Для этого выполните команду «tlntadmn config port=1000». На экране должно появиться сообщение «Параметры успешно обновлены».
17. Переключитесь на компьютер client01. Вернитесь в окно с командной строкой.
18. Выполните команду «telnet 192.168.0.12 1000». Должно появиться приветствие программы-клиента Microsoft Telnet. На вопрос «Вы намерены передать информацию .....Послать в любом случае (y/n):» введите n и нажмите «Enter». На запрос «login:» введите user3. На запрос «password:» введите P@ssw0rd. После появления сообщения «Вас приветствует Telnet-сервер.» введите команду exit. Нам удалось подключиться к Telnet-серверу на порт 1000, не меняя настроек брандмауэра.

6.7. Закрепление материала

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

1. Какие компоненты безопасности ОС контролируются Центром обеспечения безопасности?

2. Как изменяется режим работы Центра обеспечения безопасности при подключении компьютера к домену?

3. Как Центр обеспечения безопасности определяет состояние контролируемых им компонентов?

4. Какой трафик контролирует встроенный брандмауэр Windows?
   a) Только входящий;
   b) Только исходящий;
   c) Входящий и исходящий;
   d) Только не проверенный антивирусом.

5. Как можно настроить брандмауэр Windows для разрешения входящих соединений заданной программы, использующей порт UDP 15000?

6. Какие два профиля существуют для настройки брандмауэра Windows через групповую политику?

1. Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2. Microsoft, April 2005, 59 с. (http://www.microsoft.com/downloads/details.aspx?FfamilyID=4454e0e1-61fa-447a-bdcd-

Тема: Встроенная защита в Windows от вредоносного ПО Windows Defender

СОДЕРЖАНИЕ

7. Встроенная защита в Windows Vista от вредоносного ПО Windows Defender

В этом занятии будет рассмотрен «Защитник Windows» (Windows Defender). Этот продукт предлагается Microsoft как технология безопасности, защищающая компьютер от программ-шпионов и других видов нежелательных программ [1]. Предполагается, что этот программный продукт будет интегрирован в Windows Vista, а для пользователей Windows XP этот продукт будет доступен в виде отдельного дополнения [2]. На момент создания данного занятия, на сайте Microsoft доступна бета-версия 2, сборка 1347 этого продукта на английском, немецком и японском языках. После бета-тестирования программа будет переведена на другие языки [3]. Всё дальнейшей описание базируется на возможностях английской версии этой программы.

кде всего

Для изучения материалов этого занятия необходимо:

- компьютер под управлением операционной системы Windows XP Professional с настройками по умолчанию.
- выход в Интернет.

7.1. Введение

Microsoft предлагает следующее определение для «шпионского» ПО [4]:

«Шпионскими» называются программы, выполняющие определенные действия (например, показ рекламы, сбор личной информации или изменение настроек компьютера) без ведома и контроля пользователя.

Как указывается в [4,5], вероятными признаками наличия на вашем компьютере «шпионского» либо иного нежелательного программного обеспечения являются:

- Появление всплывающей рекламы, даже когда Вы не находитесь в Интернете.
- Домашняя страница или настройки поиска в обозревателе изменились без вашего ведома.
- Появление в обозревателе новых ненужных панелей инструментов, от которых трудно избавиться.
- Неожиданное значительное снижение производительности.
- Количество сбоев в работе компьютера неожиданно увеличилось.

Как указывается в [5], некоторые из программ-шпионов могут также выполнять следующее:

- регистрировать нажатия клавиш, что позволяет программам-шпионам перехватывать пароли и данные для входа в систему;

• собирать личные данные, такие как идентификационные номера, номера социального страхования (в США) или информацию о банковских счетах, и пересылать их третьим лицам;

• позволять удаленно управлять компьютером для получения доступа к файлам, установки и изменения программного обеспечения, а также использования компьютера для распространения вирусов и других действий.

Все формы программ-шпионов обладают одним общим признаком: они устанавливаются без ведома пользователя и не предоставляют ему сведений о своих действиях [5].

Для защиты от программ-шпионов и вирусов, компания Microsoft предлагает следующие технологии [1,2]:

• Защитник Windows (Windows Defender) (бета-версия 2) - инструмент защиты от «шпионского» ПО. Осуществляет не только поиск и удаление «шпионского» ПО, но и постоянный мониторинг действий пользователя и приложений с целью обнаружения попыток установки на компьютер нежелательного ПО. Основан на технологиях компании GIANT Company Software Inc., приобретенной Microsoft в декабре 2004 года [5,2].

• Windows Live Safety Center — веб-служба, обеспечивающая нормальную работу компьютера благодаря средствам сканирования, удаления нежелательных программ. Также позволяет выполнять резервное копирование файлов и дефрагментацию жестких дисков.

• Средство удаления вредоносных программ (Malicious Software Removal Tool) — средство безопасности, которое проверяет компьютер и удаляет обнаруженные вирусы и другие вредоносные программы. Основано на технологиях приобретенной Microsoft в июне 2003 года румынской антивирусной компании GeCAD.

• Windows Live OneCare - набор средств безопасности, которые почти не требуют вашего вмешательства в своей работе. Помимо антивирусной защиты, осуществляет на компьютере пользователя действия, необходимые для повышения производительности и для обеспечения сохранности данных (управление брандмауэром, резервное копирование, дефрагментация жестких дисков).

• Microsoft Client Protection - средство защиты рабочих, переносных компьютеров и файловых серверов от таких угроз, как программы-шпионы и rootkit, а также от вирусов и других традиционных способов атаки. В отличие от OneCare, данный продукт не содержит брандмауэра, средств мониторинга производительности и инструментов резервного копирования.

В табл. 7.1 приведены сравнительные характеристики перечисленных выше технологий защиты Microsoft от программ-шпионов и вирусов [1].

Таблица 7.1

Сравнение технологий защиты Microsoft от программ-шпионов и вирусов

Название продукта и целевые пользователи	**Сдерживание программ-шпионов и других нежелательных программ**		**Сдерживание вирусов и вредоносного ПО**		**Сканирование по расписанию**	**Предоставляется без дополнительной платы**
	Сканирование и удаление	Защита	Сканирование и удаление	Защита		
Защитник Windows (**бета- версия** 2) (**клиенты**)						
Windows Live Safety Center (**клиенты**)						
Malicious Software Removal Tool (**клиенты и предприятия**)						
Windows Live OneCare (**клиенты**)						
Microsoft Client Protection (**предприятия**)						

7.2. Установка Windows Defender

Для установки программы вам необходимы права администратора на локальном компьютере. Процесс инсталляции очень прост и после окончания не требует перезагрузки компьютера.

После установки, для запуска программы достаточно привилегий обычного пользователя, но некоторые действия могут требовать привилегий администратора.

7.2.1. Требования к системе

Как указывается в [6], минимальными требованиями для установки являются:

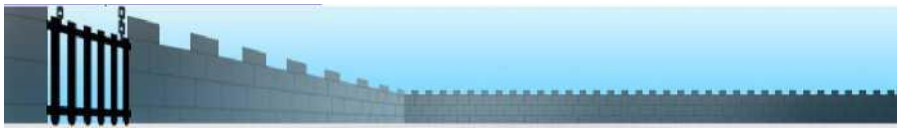
•Процессор -Intel Pentium с частотой не менее 233 МГц. Рекомендуется Pentium III.

•Операционная система: Microsoft Windows 2000 с пакетом обновления 4 (SP4) или более поздним, Windows XP с пакетом обновления 2 (SP2) или более поздним, Windows Server 2003 с пакетом обновления 1 (SP1) или более поздним.

- ОЗУ: не менее 64 МБ; рекомендуется 128 МБ.
- 20 МБ свободного места на жестком диске.
- Microsoft Internet Explorer 6.0 или выше.
- Подключение к Интернету со скоростью не менее 28,8 Кбит/с.
- Windows Installer версии 3.1 или выше.

7.2.2. Шаг 1. Загрузка Защитника Windows

Для установки приложения необходимо загрузить установщик с веб-узла центра загрузки Microsoft [7]. Для этого на «Домашней странице Защитника Windows» [3] щелкните по надписи «Загрузить здесь» (рис. 7.1).



Защитник Windows (бета-версия 2) Бесплатная **защита от** программ-шпионов.

► ЗАГРУЗИТЬ ЗДЕСЬ
Более 25 миллионов активных пользователей

Защитник Windows (бета-версия [illegible] доставляется бесплатно. Он позволяет защитить систему от всплы[illegible]н, снижения производительности и угроз бе[illegible] вызванных программами.

Рис. 7.1. Фрагмент домашней страницы Защитника Windows Защитник Windows является бесплатной программой для владельцев лицензионно чистой версии Windows. Поэтому на появившейся странице, перед загрузкой установщика, вам предлагается проверить подлинность вашей версии Windows. Об этом свидетельствует надпись «Validation Required» на странице загрузки (рис. 7.2) [7].

Windows® Defender (Beta 2)

xS6 **w**

: **aRfWindows**

Brief Description

On This Page
Quick Details
^ System Requirements

Overview
Instructions
What Are
Others

C

Validation Required

This download is available to customers running genuine Microsoft Windows. Please click the Continue button to begin Windows [illegible]

Рис. 7.2. Фрагмент страницы загрузки Защитника Windows Нажмите кнопку «Continue» для проверки операционной системы вашего компьютера. После этого вы перейдете на страницу установки компонента проверки подлинности Windows (the Genuine Windows Validation Component) (рис. 7.3). Этот компонент является элементом управления ActiveX под названием «Windows Genuine Advantage». В соответствии с настройками по умолчанию, в Internet Explorer (версия, входящая в состав Windows XP SP2) запрещена автоматическая установка элементов ActiveX. Об этом свидетельствует появившаяся панель информации со значком

Для продолжения установки необходимо выполнить щелчок левой кнопкой мыши по этой панели (рис. 7.3). В появившемся меню (рис. 7.4) выберите команду «Установить элемент управления ActiveX...».

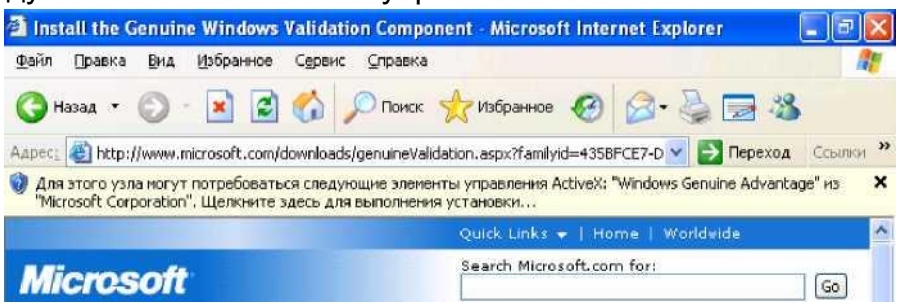


Рис. 7.3. Страница установки компонента проверки подлинности Windows

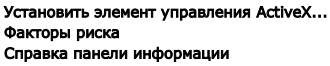


Рис. 7.4. Меню панели информации

После появления предупреждения системы безопасности об установке ActiveX компонента, нажмите кнопку «Установить» (рис. 7.5).

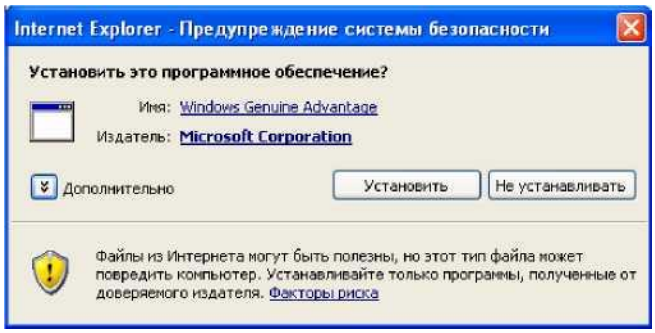


Рис. 7.5. Предупреждение системы безопасности

После успешной проверки вашей операционной системы, вы вернетесь на страницу загрузки Защитника Windows. Но внешний вид этой страницы теперь будет другой. Вместо кнопки «Continue» (рис. 7.2) будет кнопка «Download» (рис. 7.6).

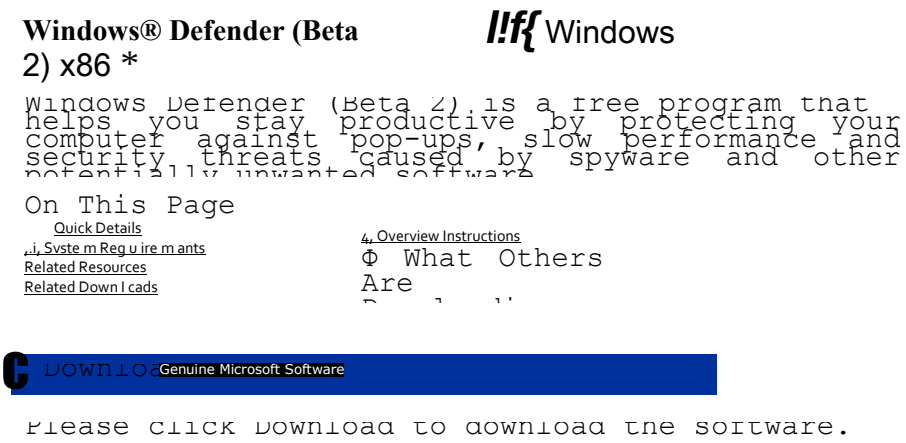


Рис. 7.6. Страница загрузки Защитника Windows после проверки ОС

Выберите язык интерфейса Защитника Windows с помощью параметра «Change Language» и нажмите кнопку «Download» (рис. 7.7). Как было указано ранее, на момент написания этого текста существовали версии Защитника Windows только на английском, немецком и японском языках.

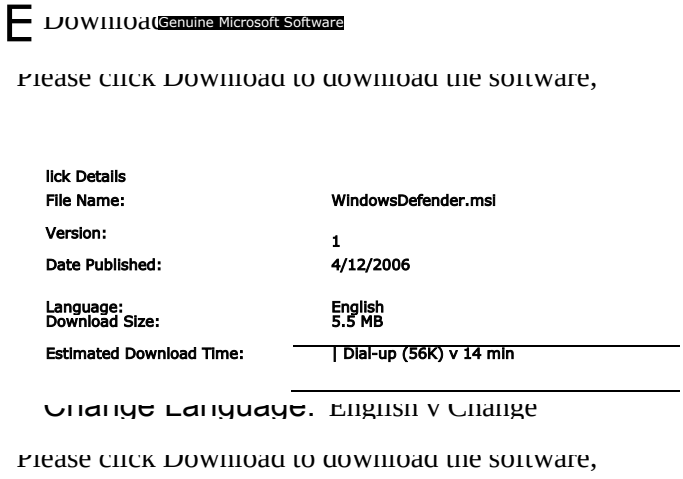


Рис. 7.7. Краткая информация о загружаемом файле После появления предупреждения системы безопасности, нажмите кнопку «Сохранить» (рис. 7.8) и выберите место для сохранения файла `WindowsDefender.msi`. Если во время установки Защитника Windows возникнут ошибки, вы всегда сможете запустить установку повторно, если сохраните установщик на диск.

Рис. 7.8. Предупреждение системы безопасности

7.2.3. Шаг 2. Запуск установщика Защитника Windows

После того как вы загрузили на свой компьютер установщик Защитника Windows, можно приступать к собственно установке. Запустите файл `WindowsDefender.msi`. Если после запуска вы увидите окно приветствия Мастера установки (см. рис. 7.9), то перейдите к шагу 5 (пункт 7.2.6). Если вы увидите сообщение об отсутствии Windows Installer 3.1 представленное на рис. 7.10, то перейдите к пункту 7.2.4. Если вы увидите сообщение о необходимости обновления службы Windows Update представленное на рис. 7.11, то перейдите к пункту 7.2.5.

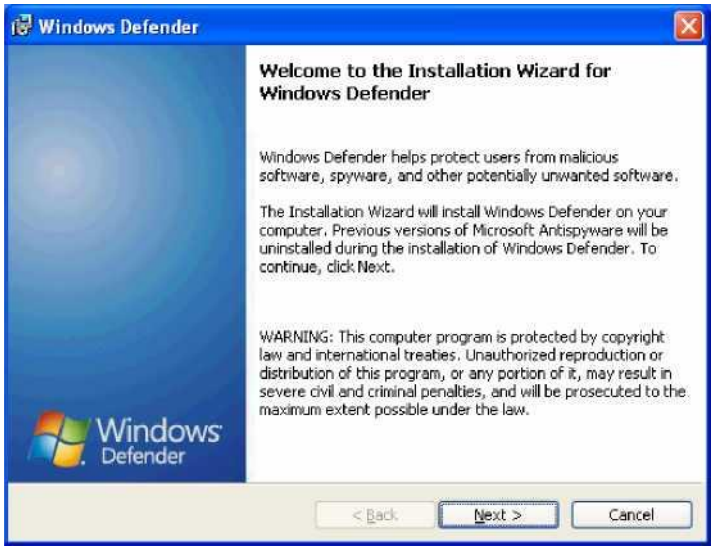


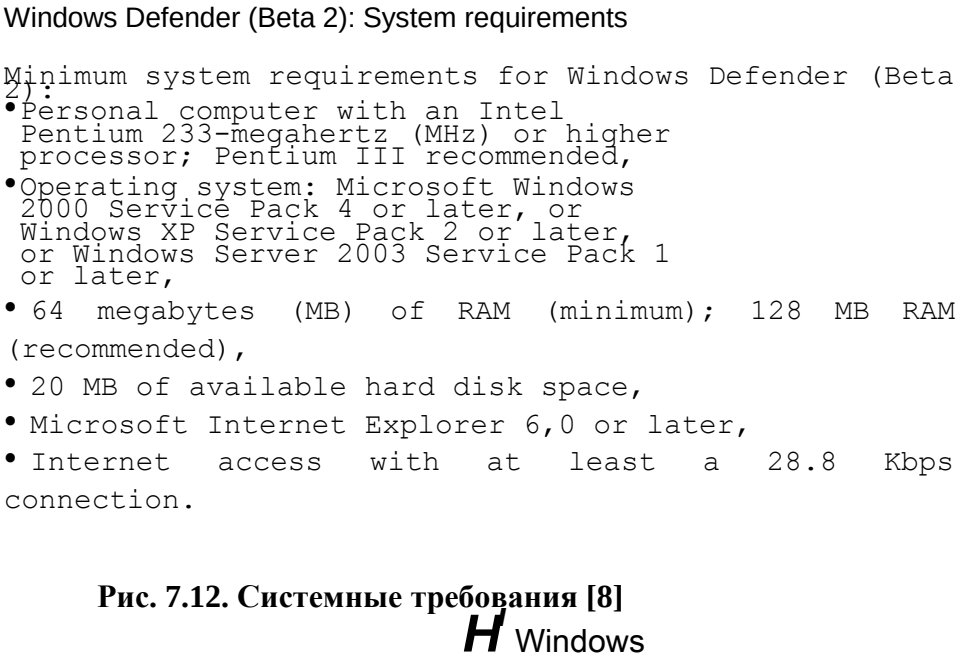
Рис. 7.9. Приветствие Мастера установки

Рис. 7.10. Сообщение об отсутствии Windows Installer 3.1

Рис. 7.11. Сообщение о необходимости обновить службу Windows Update

7.2.4. Шаг 3. Установка Windows Installer 3.1

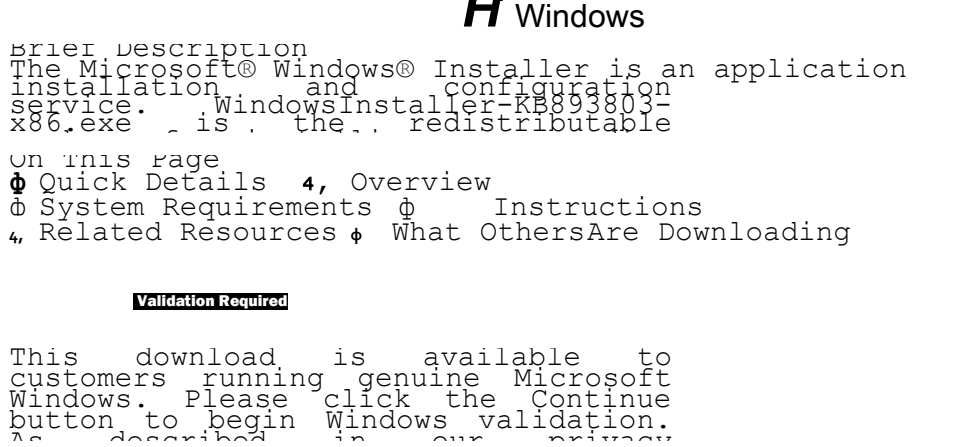
Как указано на рис. 7.10 для установки Защитника Windows необходимо наличие на компьютере приложения Windows Installer версии 3.1 или выше. Чтобы получить подробные требования к установке, необходимо посетить сайт http://go.microsoft.com/fwlink/?LinkId=63848 (рис. 7.12). Кроме описанных ранее системных требований, на этой странице есть также ссылка на Microsoft Download Center (рис. 7.12). Перейдя по этой ссылке, вы получите возможность скачать на свой компьютер Windows Installer последней версии (рис. 7.13).


Windows Defender (Beta 2): System requirements

Minimum system requirements for Windows Defender (Beta 2):

- Personal computer with an Intel Pentium 233-megahertz (MHz) or higher processor; Pentium III recommended,
- Operating system: Microsoft Windows 2000 Service Pack 4 or later, or Windows XP Service Pack 2 or later, or Windows Server 2003 Service Pack 1 or later,
- 64 megabytes (MB) of RAM (minimum); 128 MB RAM (recommended),
- 20 MB of available hard disk space,
- Microsoft Internet Explorer 6,0 or later,
- Internet access with at least a 28.8 Kbps connection.

Рис. 7.12. Системные требования [8]


H Windows

Brief Description
The Microsoft® Windows® Installer is an application installation and configuration service. WindowsInstaller-KB893803-x86.exe is the redistributable

On this Page
Quick Details Overview
System Requirements Instructions
Related Resources What OthersAre Downloading

Validation Required

This download is available to customers running genuine Microsoft Windows. Please click the Continue button to begin Windows validation.

Рис. 7.13. Страница загрузки Windows Installer 3.1 Как вы видите на рис. 7.13, для загрузки Windows Installer 3.1 также требуется проверка подлинности операционной системы. Эта проверка выполняется аналогично описанной ранее на шаге 1 (см. п. 7.2.2). После её выполнения загрузите файл WindowsInstaller-KB893803-v2-x86.exe и запустите его. Следуйте инструкциям Мастера установки. По окончании установки, не забудьте перезагрузить компьютер.

Вернитесь к шагу 2 (п. 7.2.3) и попробуйте повторно начать установку Защитника Windows.

7.2.5. Шаг 4. Обновление службы Windows Update

Как указано на рис. 7.11, для установки Защитника Windows необходимо обновить на вашем компьютере службу Windows Update. Для этого запустите Internet Explorer и выполните команду меню «Сервис | Windows Update» или перейдите по адресу «http://windowsupdate.microsoft.com/». Через несколько секунд вы увидите предупреждение системы безопасности с предложением установить приложение Windows Update (рис. 7.14). Нажмите кнопку «Установить». Если после установки потребуется переза-

грузка - выполните её. Вернитесь к шагу 2 (п. 7.2.3) и попробуйте повторно начать установку Защитника Windows.

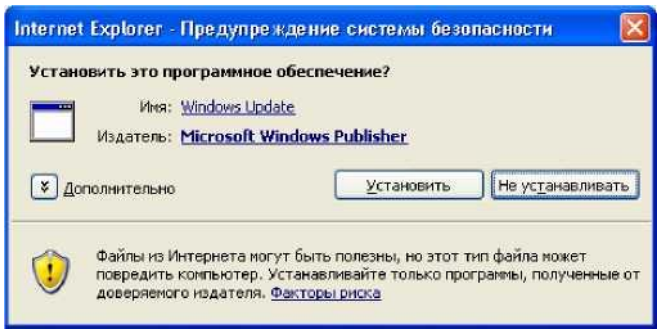


Рис. 7.14. Предупреждение системы безопасности

7.2.6. Шаг 5. Мастер установки Защитника Windows

После появления на экране окна приветствия Мастера установки (рис. 7.9), нажмите кнопку «Next». Прочтите лицензионное соглашение (рис. 7.15). Если Вы его принимаете, то выберите «I accept the terms in the license agreement» и нажмите кнопку «Next».

Рис. 7.15. Лицензионное соглашение

На следующей странице Вам будет предложено вступить в сообщество Microsoft SpyNet (рис. 7.16). Microsoft рекомендует выбрать первый вариант («Use recommended settings») [9]. В этом случае вы будите автоматически получать обновления информации о «шпионских» программах и вступите в сообщество Microsoft SpyNet.

Рис. 7.16. Предложение вступить в сообщество Microsoft SpyNet

Сообщество Microsoft SpyNet (или сеть голосования) позволяет входящим в неё пользователям получать информацию о программах, которые были запрещены, удалены или разрешены другими пользователями при работе с Защитником Windows. Кроме того, ваши решения по этому вопросу также будут доступны другим пользователям. Данные о решениях пользователей отображаются в Защитнике Windows (бета-версия 2) в виде графика, который содержит информацию о процентном соотношении людей, разрешивших, запретивших или удаливших конкретную программу [10].

Если вы не хотите вступать сообщество Microsoft SpyNet, но желаете получать обновления информации о «шпионских» программах, то выберите вариант «Install definition updates only».

При выборе варианта «Ask me later» вы не будете получать обновления и вступать в сообщество Microsoft SpyNet.

Выберите первый вариант и нажмите кнопку «Next». На следующей странице вам будет предложено выбрать тип установки: полная («Complete») или выборочная («Custom») (рис. 7.17). Выберите вариант «Complete» и нажмите кнопку «Next».

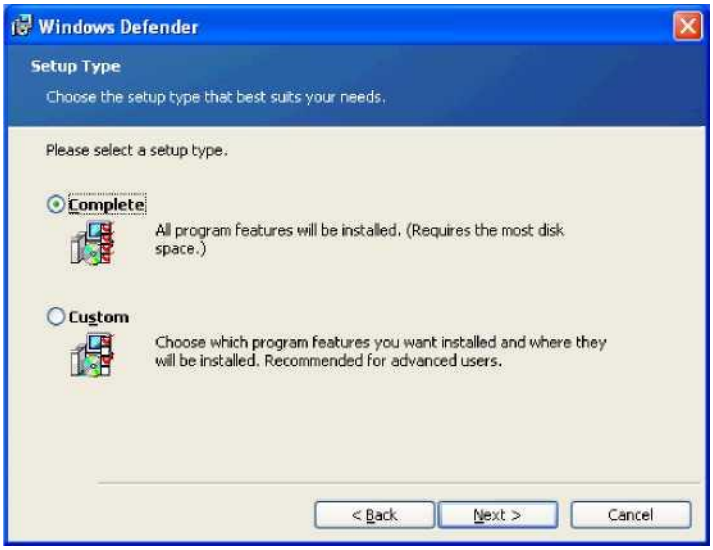


Рис. 7.17. Выбор типа установки

На следующем экране вам будет сообщено о готовности к установке Защитника Windows (рис. 7.18). Нажмите кнопку «Install».

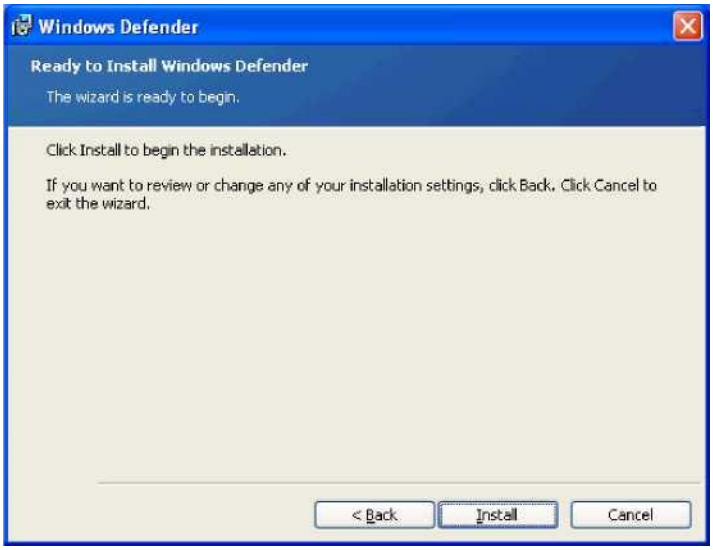


Рис. 7.18. Готовность к установке

После завершения установки появится соответствующая страница с предложением проверить наличие обновлений информации о «шпионских» программах и запустить быстрое сканирование вашего компьютера (рис. 7.19). Нажмите кнопку «Finish».

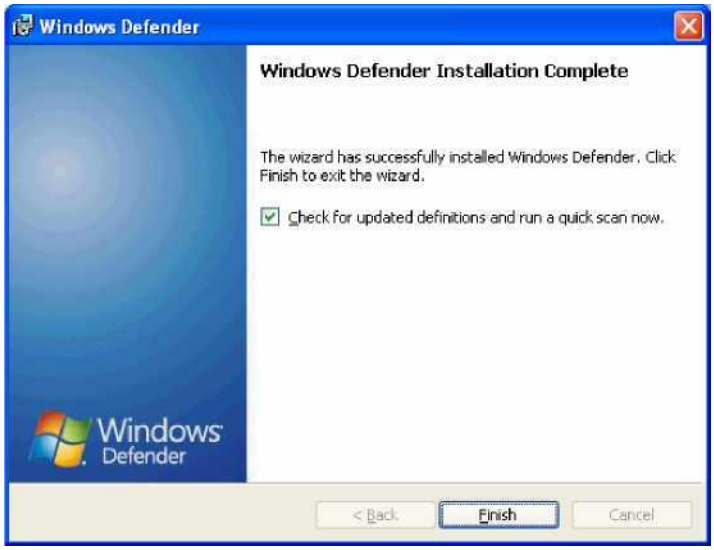


Рис. 7.19 Успешное завершение установки Для запуска Защитника Windows в меню «Пуск» выберите пункт «Все программы», а затем - пункт «Windows Defender» (Защитник Windows) (рис. 7.20).

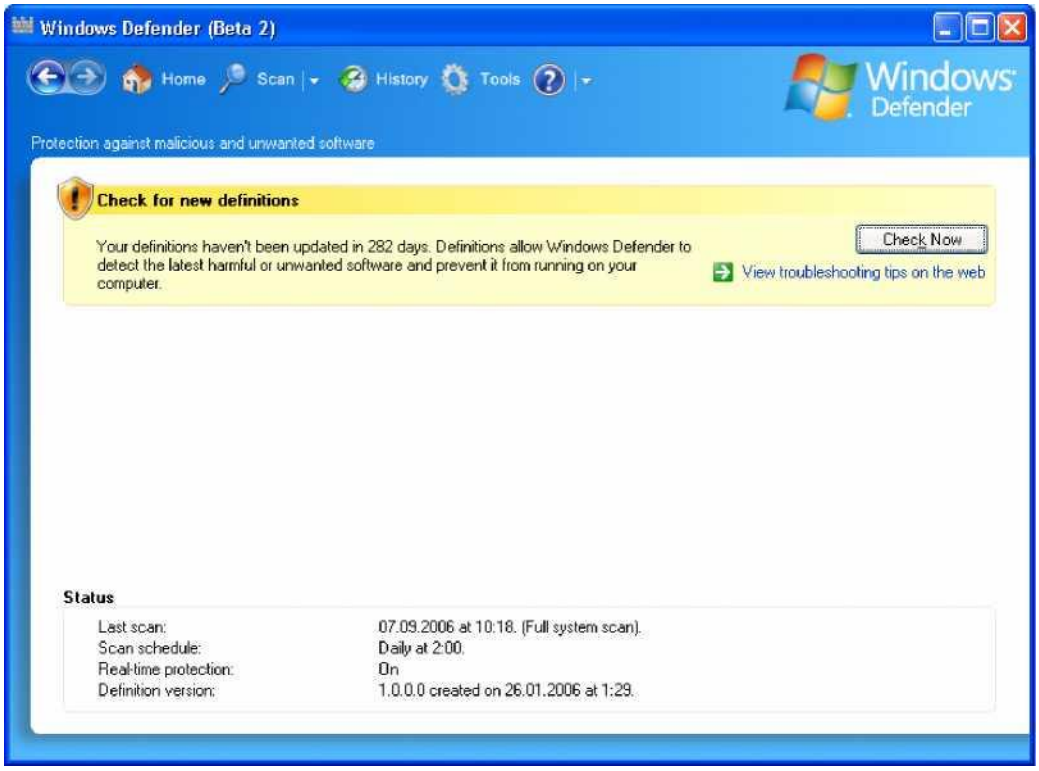


Рис. 7.20 Главное окно Защитника Windows.

7.3. Настройки Windows Defender

Для просмотра и изменения параметров работы Защитника Windows на панели инструментов выберите «Tools» (Сервис) (рис. 7.20) и в появившейся странице (см. рис. 7.21) выберите пункт «Options».

Рис. 7.21 Страница «Tools» (Сервис)

Настройки Защитника Windows состоят из пяти разделов:

- Automatic scanning (автоматическое сканирование) (рис. 7.22).
- Default actions (действия по умолчанию) (рис. 7.23).
- Real-time protection options (настройки постоянной защиты или защита в реальном времени) (рис. 7.24).
- Advanced options (расширенные настройки) (рис. 7.25).
- Administrator options (настройки Администратора) (рис. 7.26).

Если Вы измените любой из параметров, то для сохранения этих изменений, необходимо нажать кнопку «Save» внизу экрана.

Рассмотрим каждый из этих разделов более подробно.

7.3.1. Automatic scanning (автоматическое сканирование)

В этом разделе сосредоточены настройки планирования проверки компьютера на наличие программ-шпионов и других потенциально нежелательных программ. Параметр «Automatically scan my computer (recommended)» (Автоматически сканировать мой компьютер [рекомендуется]) позволяет включить автоматическую проверку компьютера (рис. 7.22).

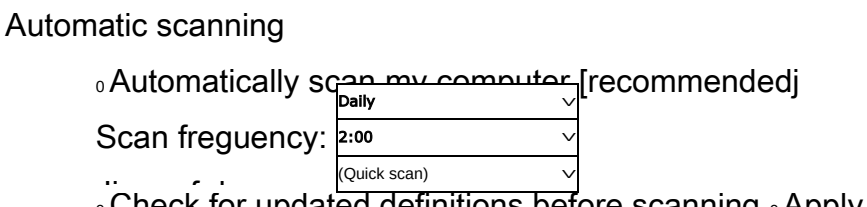


Рис. 7.22 Настройки автоматического сканирования

Параметр «Scan frequency:» (частота сканирования) позволяет задать периодичность автоматического сканирования. Доступны варианты: «Daily» (ежедневно), «Понедельник», «Вторник», ..., «Воскресенье».

Параметр «Time of day:» (время дня) определяет время начала сканирования.

Параметр «Type of scan:» (тип сканирования) позволяет выбрать, какая проверка будет выполняться: «Quick scan» (быстрая проверка) или «Full system scan» (полная проверка системы). При быстрой проверке проверяются те области компьютера, которые наиболее подвержены воздействию нежелательного программного обеспечения. При полной проверке системы проверяются все файлы на жестком диске и все выполняемые в данный момент программы. При этом возможно замедление работы компьютера до завершения сканирования. Microsoft рекомендует запланировать ежедневную быструю проверку, а в случае подозрения на заражение компьютера программами-шпионами - выполнять полную проверку системы [11].

Параметр «Check for updated definitions before scanning» позволяет перед сканированием компьютера проверить наличие обновлений информации о нежелательных программах на сервере обновлений Windows.

Параметр «Apply default actions to items detected during a scan» позволяет при обнаружении нежелательного программного обеспечения выполнять действия по умолчанию заданные в следующем разделе (см. след. пункт). Если этот параметр выключен, то при обнаружении программ- шпионов и других потенциально нежелательных программ Защитник Windows будет запрашивать у пользователя что необходимо сделать с обнаруженным подозрительным объектом.

7.3.2. Default actions (действия по умолчанию).

В этом разделе Вы можете определить, какие действия необходимо выполнять при обнаружении подозрительных объектов (рис. 7.23). Для различных типов предупреждений (high - высокий, medium - средний, low - низкий) вы можете задать свой вариант реагирования. Доступны следующие варианты:

• Definition recommended action (установлено рекомендованное действие).

• Ignore (игнорировать подозрительный объект и разрешить ему выполняться).

• Remove (удалить объект и не допустить его выполнение).

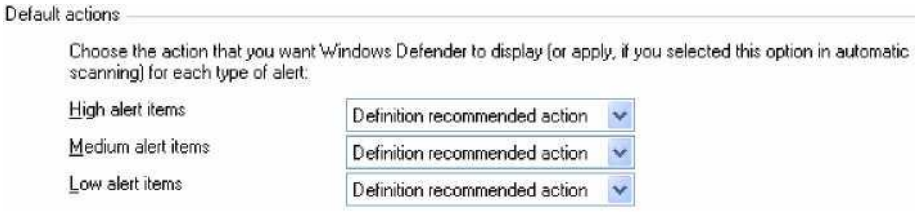


Рис. 7.23 Действия по умолчанию

7.3.3. Real-time protection options (настройки постоянной защиты).

В этом разделе находятся настройки связанные с защитой в реальном времени (рис. 7.24).

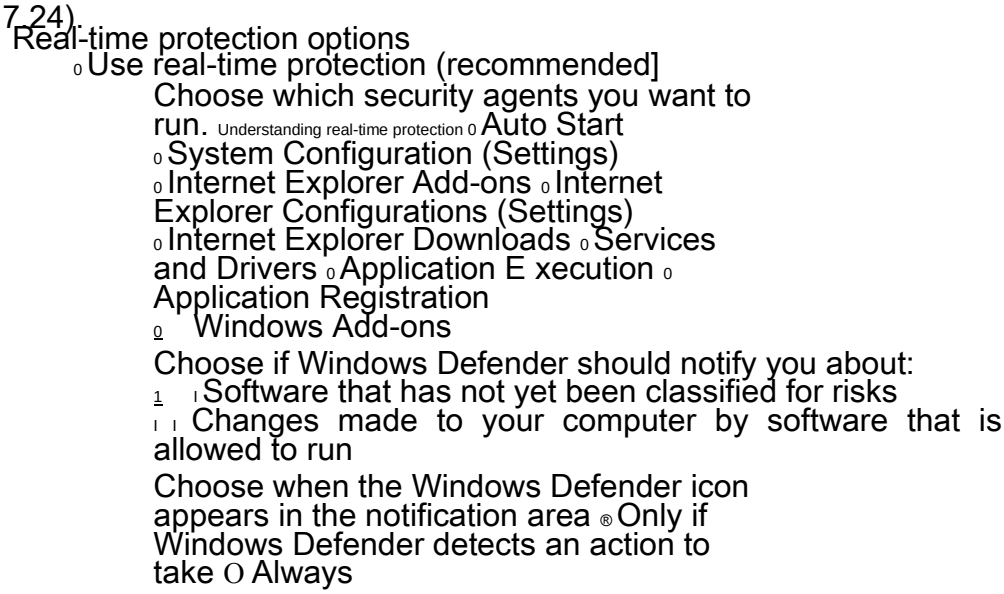


Рис. 7.24 Настройки защиты в реальном времени

Защита в реальном времени (постоянная защита) контролирует состояние важнейших компонентов операционной системы (ОС). Когда посторонние программы производят изменения в настройках ОС или пытаются установиться на компьютер, защита в реальном времени фиксирует эти действия и уведомляет об этом пользователя [10].

Параметр «Use real-time protection (recommended)» (использовать защиту в реальном времени [рекомендуется]) позволяет включить или выключить постоянную защиту.

Ниже перечислены агенты безопасности, контролирующие различные компоненты ОС. Вы можете включить или выключить нужные Вам компоненты, но Microsoft рекомендует не выключать защиту в реальном времени и использовать все существующие агенты безопасности. В табл. 7.2. представлено назначение каждого агента, взятое из встроенной помощи Защитника Windows.

Таблица 7.2

Агенты безопасности защиты в реальном времени

Агент	Назначение
Auto Start	Контроль списка программ автоматически запускающихся при старте компьютера
System Configuration (settings)	Контроль настроек связанных с безопасностью Windows
Internet Explorer Add-ons	Контроль программ, которые автоматически запускаются при старте Internet Explorer
Internet Explorer Configurations (settings)	Контроль настроек безопасности Internet Explorer
Internet Explorer Downloads	Контроль файлов и программ, которые спроектированы для работы с Internet Explorer (например, элементы управления ActiveX и программы установки программного обеспечения из Интернета)
Services and Drivers	Контроль служб и драйверов
Application Execution	Контроль запускающихся программ и действий, которые они выполняют
Application Registration	Контроль утилит и файлов операционной системы предназначенных для запуска программ (например, по расписанию)
Windows Add-ons	Контроль дополнений (также известных как программные утилиты) для Windows

Следующие два параметра определяют, будет ли Защитник Windows уведомлять пользователя:

•о программном обеспечении, которое ещё не было классифицировано по степени риска от его использования (параметр «Software that has not yet been classified for risks»);

•об изменениях выполненных на Вашем компьютере разрешенным программным обеспечением (параметр «Changes made to you computer by software that is allowed to run»).

Следующий параметр («Choose when the Windows Defender icon appears in the notification area») определяет, когда будет появляться значок Защитника Windows в области уведомления (правая нижняя часть экрана). Вариант «Always» соответствует постоянному наличию значка. Вариант «Only if Windows Defender detects an action to take» соответствует отображению значка только в случае возникновения какого-либо события. Например, когда Защитник Windows давно не соединялся с сервером обновлений Windows и не скачивал новые описания нежелательных программ.

7.3.4. Advanced options (расширенные настройки)

В этом разделе (рис. 7.25) находятся следующие параметры, название которых говорит само за себя:

•«Scan the contents of archived files and folders for potential threats» (сканировать содержимое архивных файлов и папок в поисках потенциальной угрозы). К сожалению, в справке Защитника Windows отсутствует информации о типах поддерживаемых архивов.

•«Use heuristics to detect potentially harmful or unwanted behavior by software that hasn’t been analyzed for risks» (использовать эвристический анализ для обнаружения потенциально опасных или нежелательных про

грамм, которые ещё не были проанализированы разработчиком Защитника Windows).

• «Do not scan these files or location» (не сканировать указанные файлы или папки). Для задания списка файлов или папок, не подлежащих проверке, нажмите кнопку «Add...». Кнопка «Remove» позволяет удалить из этого списка ранее указанные файлы или папки.

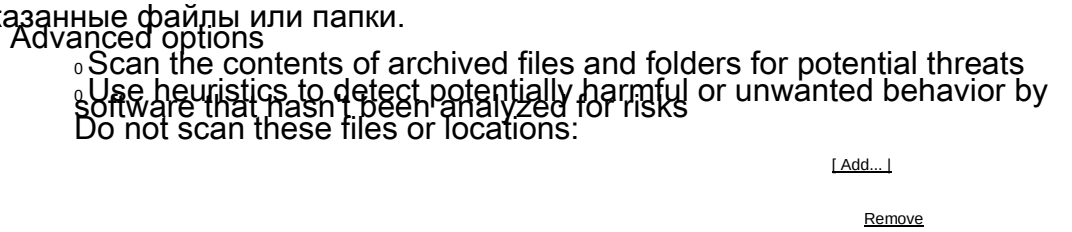


Рис. 7.25 Расширенные настройки

7.3.5. Administrator options (настройки Администратора)

В этом разделе (рис. 7.26) находятся следующие настройки:

• «Use Windows Defender» (включить Защитника Windows). Если этот параметр включен - все пользователи будут получать предупреждения в случае обнаружения шпионского ПО или выполнения нежелательных действий. Защитник Windows будет периодически проверять наличие обновлений на сервере обновлений Windows, регулярно проверять Ваш компьютер и автоматически удалять нежелательное ПО обнаруженное при сканировании.

• «Allow users to use Windows Defender» (разрешить пользователям использовать Защитник Windows). Если этот параметр включен, пользователи, не обладающие административными привилегиями, смогут взаимодействовать с Защитником Windows.

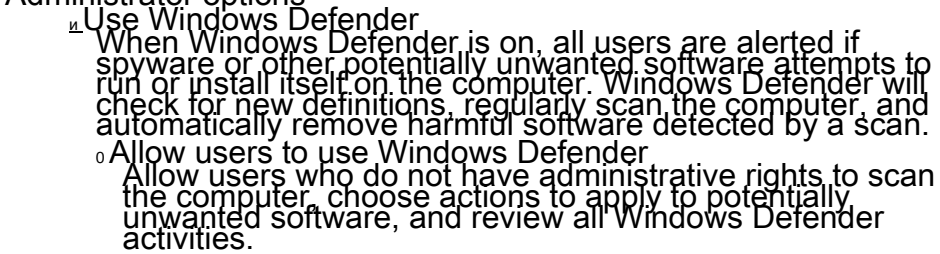


Рис. 7.26 Настройки Администратора

7.4. Обновление Windows Defender

Защитник Windows работает тем эффективнее, чем большей информацией о существующих в мире шпионских и прочих нежелательных программах он обладает. Эту информацию Windows Defender получает с сервера обновлений Windows (Windows Update). Соответственно, если Ваш компьютер настроен на автоматическое обновление («Пуск», «Панель управления», «Центр обеспечения безопасности», рис. 7.27) и периодиче-

ски получает обновления с сервера Windows Update, то Защитник Windows будет также получать свои обновления.

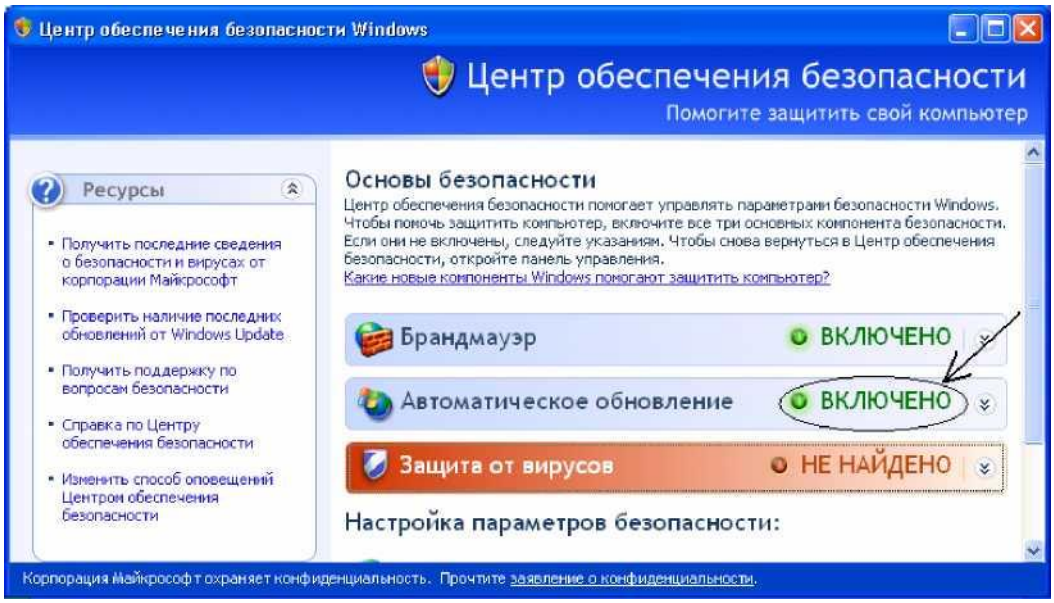


Рис. 7.27 Автоматическое обновление включено Информация о том, какая версия информационных баз сейчас используется Защитником Windows, отображается на главной странице (рис. 7.28). После установки Защитника Windows (Beta 2), версия информационных баз (Definition version) 1.0.0.0. Они созданы 26.01.2006 (рис. 7.28). Если Защитник Windows считает, что базы устарели, то на главной странице появляется предупреждение (рис. 7.28).

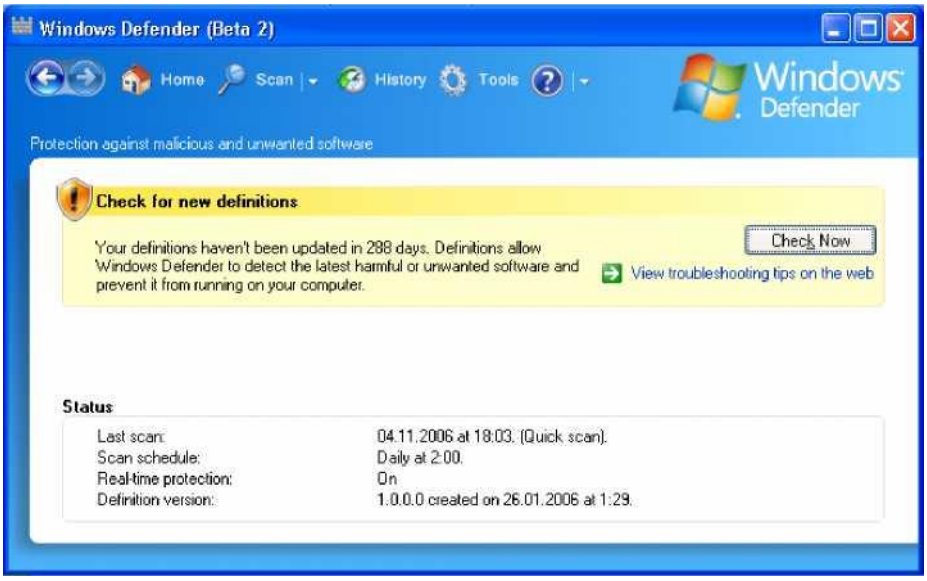


Рис. 7.28 Главная страница Защитника Windows Для того чтобы скачать свежие обновления с сервера Microsoft, нажмите кнопку «Check Now». В области уведомления (правая часть панели задач) появится значок с сообщением «Windows Defender is connecting to the Internet to acquire new definitions and engine upgrades» (рис. 7.29). Сообщение говорит о том, что Защитник Windows соединяется с Интернет для по-

лучения новых определений и обновления модуля обнаружения нежелательного ПО.

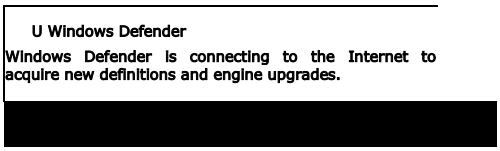


Рис. 7.29 Сообщение о соединении с Интернет

Примечание: На самом деле, если в Вашей организации развернут внутренний сервер обновлений (например, Microsoft Windows Server Update Services, WSUS) и Ваш компьютер для получения обновлений настроен на соединение с этим сервером, то Защитник Windows будет соединяться не с Интернет, а с внутренним сервером обновлений. Настройка внутреннего сервера обновлений не входит в тему данного занятия. Однако отметим, что сервер WSUS по умолчанию не скачивает из Интернета обновления определений для Защитника Windows и его необходимо соответствующим образом настраивать.

После успешного получения последних обновлений, в области уведомления появится сообщение «Windows Defender is up-to-date with definitions and engine upgrades» (Защитник Windows содержит последние определения и обновления модуля обнаружения нежелательного ПО) (рис. 7.30).

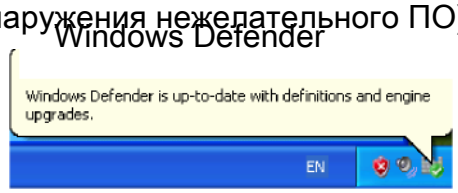


Рис. 7.30 Сообщение об успешности получения обновлений После этого, главная страница изменит своё содержание (см. рис. 7.31).

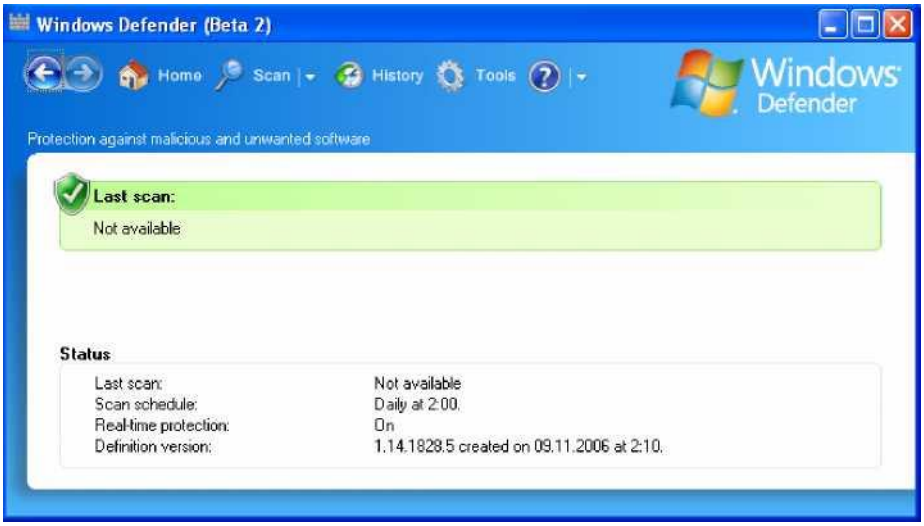


Рис. 7.31 Главная страница Защитника Windows

7.5. Проверка компьютера

Для того чтобы проверить Ваш компьютер на наличие шпионского и другого нежелательного ПО необходимо выполнить сканирование с помощью Защитника Windows. Существует три типа сканирования:

- Quick Scan (быстрое сканирование).
- Full Scan (полное сканирование).
- Custom Scan... (выборочное сканирование).

При быстрой проверке проверяются те области на жестком диске, заражение которых программами-шпионами наиболее вероятно [11]. В этом режиме проверяются не только системные папки Windows, но и важные для безопасности ветки реестра. В режиме полной проверки проверяются не только все файлы на жестком диске, но и все выполняемые в данный момент программы. Как указывается в [11], при выполнении полной проверки компьютера возможно замедление работы системы. Поэтому рекомендуется настроить Защитник Windows на ежедневную быструю проверку, а при подозрении на заражение компьютера программами-шпионами, выполнять полную проверку системы.

Выборочное сканирование позволяет провести сканирование только выбранных дисков и папок.

Для выбора нужного Вам режима сканирования компьютера, нажмите треугольник (П) рядом с кнопкой «Scan» на панели задач Защитника Windows. Если сразу нажать кнопку «Scan», то будет выполнена быстрая проверка компьютера (рис. 7.32).

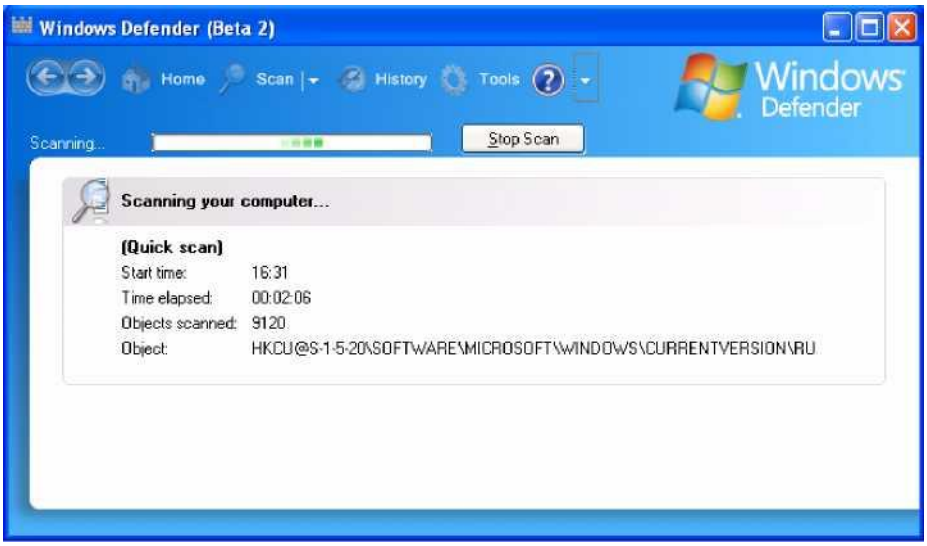


Рис. 7.32 Быстрая проверка компьютера

После её выполнения на экран будет выведена статистка проверки. На рис. 7.33 представлен результат проверки не обнаружившей подозрительных объектов.

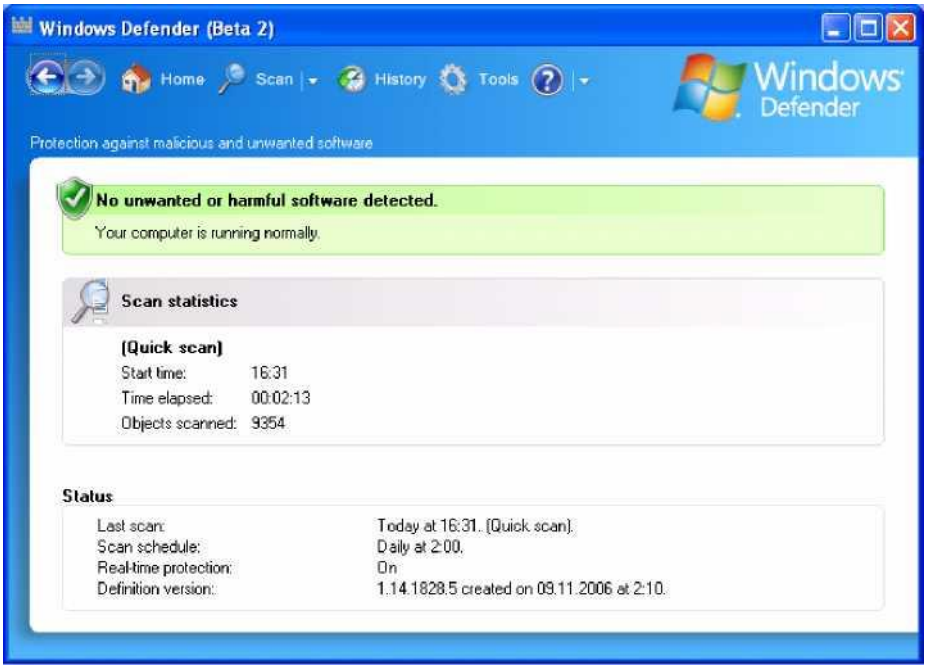


Рис. 7.33 Результат быстрой проверки

7.5.1. Обнаружение подозрительных действий

Для того чтобы получать уведомления обо всех подозрительных действиях, совершаемых на Вашем компьютере, необходимо в разделе «Choose if Windows Defender should notify you about:» включить параметр «Software that has not yet been classified for risks» (см. п. 7.3.3). В этом случае, Защитник Windows будет предупреждать Вас обо всех подозрительных действиях. Иначе (по умолчанию этот параметр выключен), он будет предупреждать Вас только о тех действиях (и тех программах), информация о которых входит в определения (definitions), созданные разработчиками Защитника Windows.

На рис. 7.34 представлено сообщение об обнаруженных подозрительных действиях. Для того чтобы узнать, что обнаружил Защитник Windows, необходимо щелкнуть по этому сообщению или дважды щелкнуть левой кнопкой мыши по значку Защитника Windows. На экране появится окно с указанием обнаруженных событий (рис. 7.35),

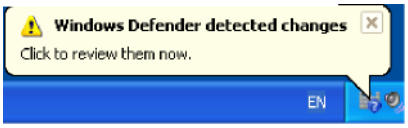


Рис. 7.34 Обнаружены подозрительные действия

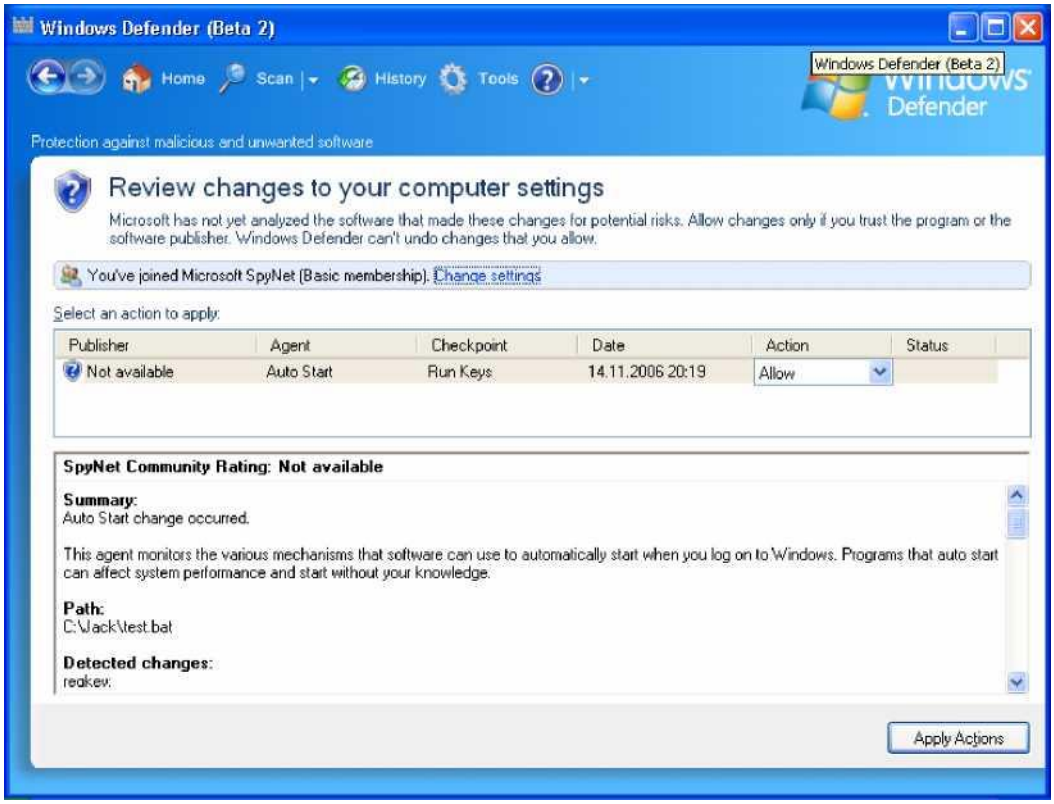


Рис. 7.35 Выбор действия

Обнаруженные события перечислены в виде таблицы в средней части экрана. В нижней части экрана, для выделенного в данный момент события, отображается более подробная информация (рис. 7.36). В разделе «Summary» отображается общая информация по событию. Далее идет более подробное описание. В разделе «Path» указывается расположение файла вызвавшего данное событие. В разделе «Detected changes» - зафиксированные в системе изменения. В разделе «Advice» дается совет: что в данном случае следует предпринять.

Summary:
Auto Start change occurred.

This agent monitors the various mechanisms that software can use to automatically start when you log on to Windows. Programs that auto start can affect system performance and start without your knowledge.

Path:
C:\Jack\test.bat

Detected changes:
regkey:
HKCU@S-1-5-21-776561741-1343024091-854245398-1004\Software\Microsoft\Windows\CurrentVersion\RunWtest.bat

runkey:
HKCU@S-1-5-21-776561741-1343024091-854245398-1004\Software\Microsoft\Windows\CurrentVersion\RunWtest.bat

file:

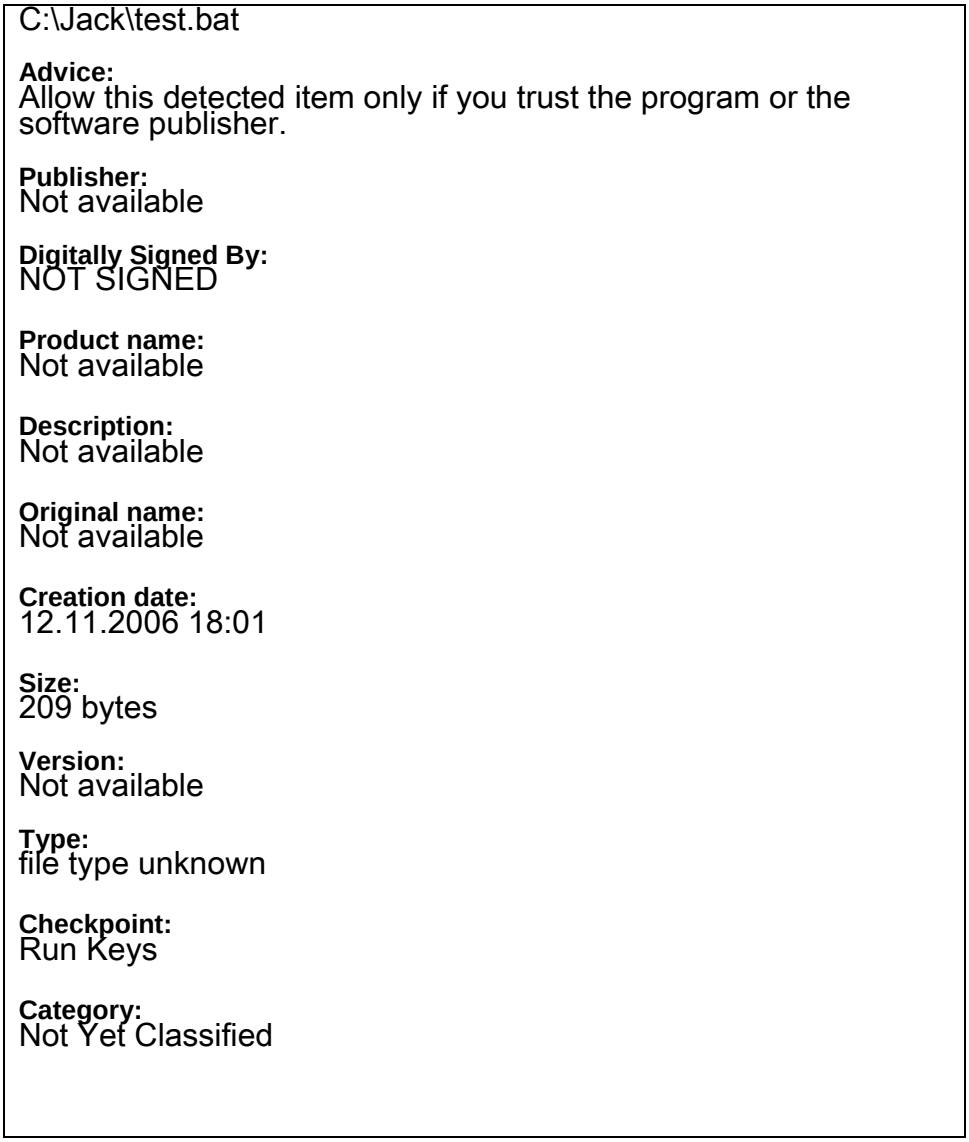


Рис. 7.36 Подробное описание подозрительного события Если Вы доверяете разработчику той программы, которая вызвала это событие, то в столбце «Action» выберите вариант «Allow» (рис. 7.35). Иначе выберите вариант «Block». В последнем случае, действия, которые были выполнены указанной программой, будут отменены. После выбора нужных действий для всех событий, нажмите кнопку «Apply Actions». Если указанное Вами действие (Block или Allow) удалось выполнить, в столбце «Status» будет выведено «Succeeded» (Рис. 7.37).

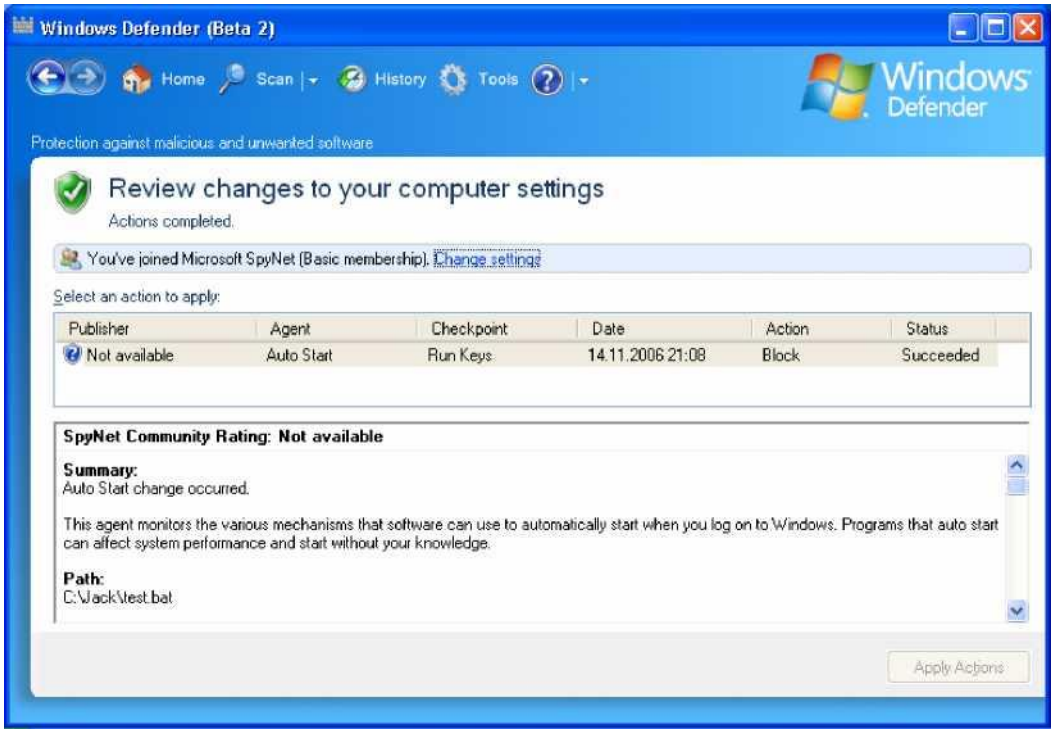


Рис. 7.37 Ваши действия были применены

7.5.2. Обнаружение программ-шпионов

В предыдущем пункте был описан пример обнаружения так называемого «не классифицируемого события». У такого события в разделе «**Category:**» (категория) отображается «Not Yet Classified» (см. рис. 7.36). По умолчанию, пользователю о таких событиях не сообщается (см. п. 7.5.1), но они фиксируются в окне «History» (История). Если информация о приложении или событии существует в информационных базах (определениях) Защитника Windows, то предупреждение о таком событии выглядит иначе (см. рис. 7.38).

Рис. 7.38 Сообщение с уровнем «Medium»

В данном случае Защитник Windows зафиксировал событие с предупреждающим уровнем (Alert level) «Medium» (средний) (рис. 7.38). Как

указывается в справке, уровни предупреждения (alert levels) помогают пользователю принять правильное решение о том, как реагировать на обнаруженное шпионское или нежелательное ПО. Не смотря на то, что Защитник Windows будет рекомендовать Вам удалить (кнопка «Remove All») программу, не все обнаруженные программы являются опасными или не желательными. В табл. 7.3 представлена информация, помогающая Вам решить что делать, если Защитник Windows обнаружил не желательное ПО на Вашем компьютере.

Таблица 7.3

Уровни предупреждения

Уровень предупреждения	Что означает	Что делать
Severe (Тяжелый**)**	Широко распространенные или исключительно опасные программы (например, вирусы или черви), которые наносят ущерб вашей личной информации и защите вашего компьютера. Эти программы могут повредить ваш компьютер.	Немедленно удалите эту программу.
High (Высокий**)**	Программы, которые могут собирать Вашу личную информацию и повредить ваш компьютер. Например, без Вашего ведома или согласия собирают информацию или меняют настройки Вашего компьютера.	Немедленно удалите эту программу.
Medium (Средний**)**	Программы, которые могут влиять на Вашу личную информацию или выполнять изменения на Вашем компьютере.	Просмотрите подробности этого предупреждения, чтобы выяснить, почему это программа была обнаружена. Если Вам не нравятся те действия, которые выполняет эта программа или Вы не доверяете разработчику этой программы, решите: заблокировать или удалить эту программу.
Low (Низкий**)**	Потенциально нежелательные программы, которые могут собирать информацию о Вас, Вашем компьютере или изменять настройки Вашего компьютера, но об этих действиях сообщается в лицензионном соглашении при их установке.	Такие программы обычно неопасны при выполнении на Вашем компьютере, если только они не были установлены без Вашего ведома. Если вы не уверены, разрешать ли работу такой программы, просмотрите подробности этого предупреждения и определите, доверяете ли Вы разработчику этой программы.
Not yet classified (не классифицируемый**)**	Обычно не опасные программы, если только они не были установлены без Вашего ведома.	Если Вы знаете эту программы и доверяете её разработчику, разрешите её выполнение. Иначе, просмотрите подробности этого предупреждения, для того чтобы принять обоснованное решение. Если Вы вступили в сообщество Microsoft SpyNet, проверьте рейтинг сети голосования, чтобы узнать доверяют ли этой программе другие пользователи.

Для того чтобы просмотреть подробности этого события, подведите курсор к строке с названием обнаруженной программы. Появится всплывающее сообщение с описанием обнаруженной программы и советом от

разработчиков Защитника Windows (рис. 7.39). Если Вы нажмете кнопку «Remove All» (Удалить Всё), то Защитник Windows попытается удалить обнаруженную программу. Об успешности этого действия можно будет судить, просмотрев окно «History» (История). Если Вы нажмете кнопку «Ignore» (Игнорировать), Защитник Windows ничего не будет делать с обнаруженной программой, о чем также появится сообщение в окне «History».

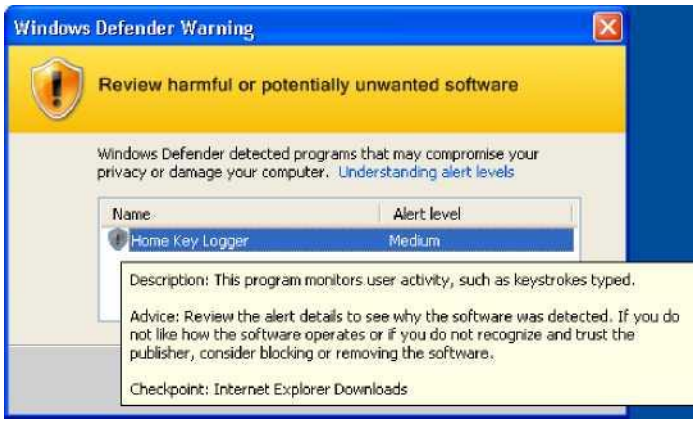


Рис. 7.39 Описание обнаруженной программы Описанный выше пример показывает реакцию Защитника Windows на операцию записи на диск программы установщика. В случае обнаружения реально работающей в данный момент (т.е. уже установленной на Вашем компьютере) программы, окно с предупреждением будет иметь дополнительную кнопку «Review» (см. рис. 7.40). При нажатии на эту кнопку появится главное окно Защитника Windows с возможностью не только удалить обнаруженную программу (кнопка «Remove All»), но и просмотреть подробности обнаруженного события (рис. 7.41). Для этого необходимо

щелкнуть ПО надписи J Review items detected by real-time protection, g результате, На ЭКране появится окно с подробным описанием события и с возможностью выбора нужного действия (рис. 7.42).

Рис. 7.40 Обнаружение исполняемой программы

Рис. 7.41 Сообщение об обнаруженном событии

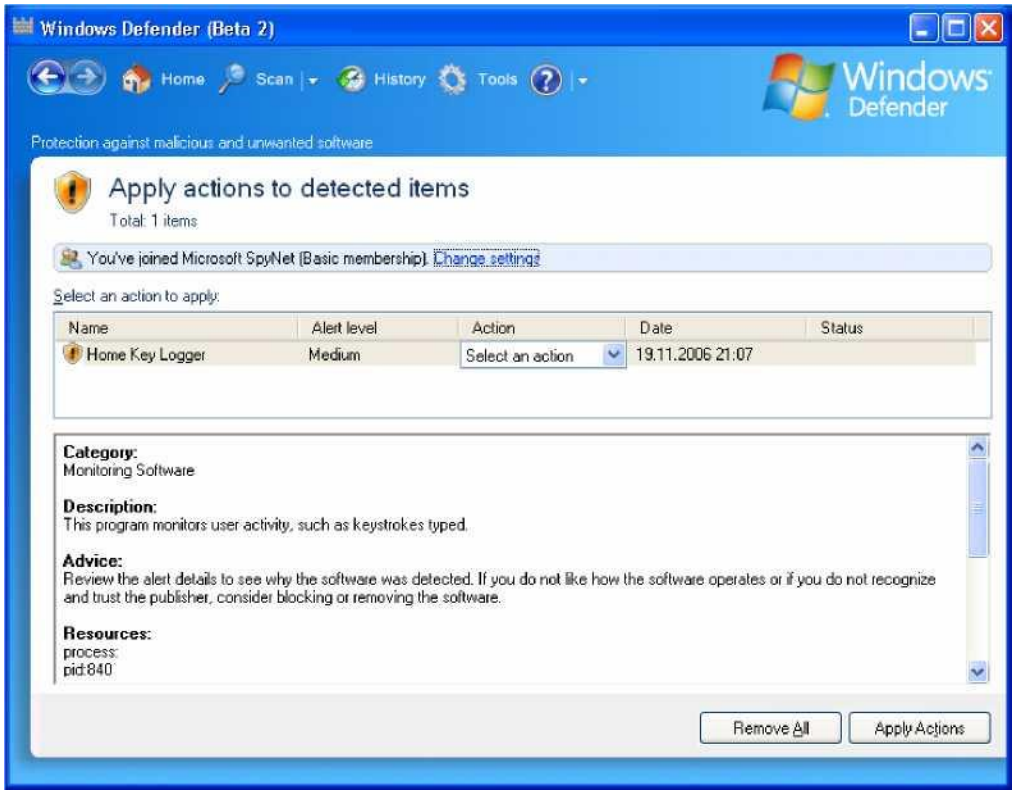


Рис. 7.42. Выберите нужное действие Возможны следующие действия:

- Ignore (игнорировать подозрительный объект и разрешить ему выполняться).
- Quarantine (переместить подозрительный объект на карантин).
- Remove (удалить подозрительный объект и не допустить его выполнение).

• Always allow (разрешить подозрительному объекту выполняться и занести его в список разрешенных программ(allowed list)).

7.5.3. Работа с карантином

При перемещении подозрительной программы на карантин, Защитник Windows перемещает её в другое место на компьютере и препятствует её работе до тех пор, пока Вы не решите удалить или восстановить её[12].

Для просмотра объектов находящихся на карантине, необходимо на панели инструментов выбрать «Tools» (Сервис) (рис. 7.20) и в появившейся странице (см. рис. 7.21) выбрать пункт «Quarantined items» (рис. 7.43).

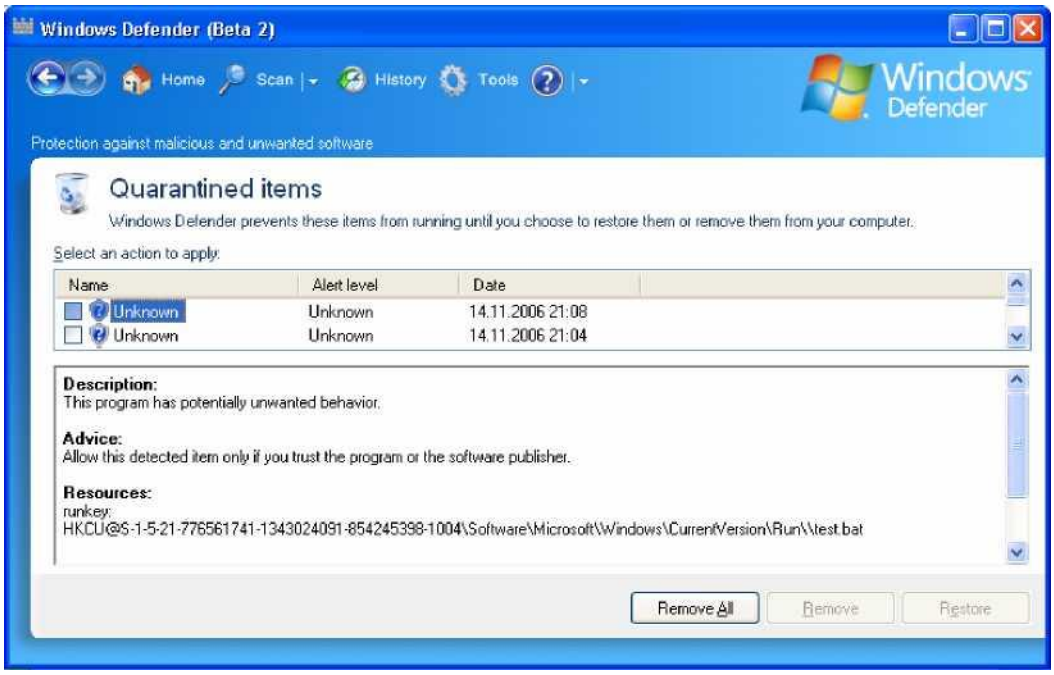


Рис. 7.43. Список объектов на карантине

Для того чтобы удалить все объекты, находящиеся на карантине, необходимо просто нажать внизу кнопку «Remove All». Для того чтобы удалить или восстановить только некоторые объекты, находящиеся на карантине, необходимо выделить их (т.е. отметить их галочками) и нажать одну из кнопок:

- Remove (удаление с компьютера выделенных объектов).
- Restore (восстановление в первоначальное местоположение выделенных объектов).

7.5.4. Работа со списком разрешенных объектов

При выборе действия «Always allow», обнаруженный объект заносится в список разрешенных программ (allowed list). Для просмотра этого списка, необходимо на панели инструментов выбрать «Tools» (Сервис) (рис. 7.20) и в появившейся странице (см. рис. 7.21) выбрать пункт «Allowed items» (рис. 7.44).

Рис. 7.44 Список разрешенных объектов

Если Вы удалите программу из этого списка, то Защитник Windows снова начнет контролировать действия, выполняемые этой программой. Для удаления программы из списка необходимо выделить её (поставить галочку) и нажать внизу кнопку «Clear».

7.5.5. Использование обозревателя программ (Software Explorer)

На странице «Tools» (см. рис. 7.21) кроме уже рассмотренных средств, присутствует утилита Software Explorer, которая позволяет просматривать подробную информацию о запущенных на компьютере программах. Эта утилита (см. рис. 7.45) помогает контролировать следующие элементы [13]:

Рис. 7.45 Обозреватель программ

• Startup Programs. Программы автозагрузки, т.е. программы, запускаемые одновременно с началом работы системы Windows. Для программ в этой категории доступны следующие действия: «Remove» - удалить, «Disable» - запретить и «Enable» - разрешить.

• Currently Running Programs. Программы, выполняемые в данный момент (отображаются на экране или работают в фоновом режиме). Для некоторых программ в этой категории доступна операция «End Process» - завершить процесс. Кроме того, существует возможность запустить диспетчер задач с помощью кнопки «Task Manager».

• Network Connected Programs. Программы, работающие с сетью. Т.е. программы или процессы, которые могут устанавливать соединение с Интернетом или другой сетью. Для программ в этой категории доступны следующие действия: «End Process» - завершить процесс, «Block Connection» - заблокировать соединение.

• Winsock Service Provider. Поставщики услуг Winsock. Это программы, которые обеспечивают низкоуровневые сетевые службы и службы связи для систем Windows и программ, работающих с Windows[13].

Примечание: Чтобы воспользоваться некоторыми функциями обозревателя программ, нужно обладать правами Администратора.

В зависимости от выбранной категории, по каждой программе в Software Explorer можно просмотреть следующие сведения (см. табл. 7.4).

Таблица 7.4

Сведения, отображаемые в обозревателе программ [13]

| **Параметр** | **Описание** |

Auto Start (Автозагрузка)	Показывает, зарегистрирована ли программа для автоматического запуска при запуске операционной системы.
Startup Type (Тип запуска)	Адрес регистрации программы для автоматического запуска (реестр или папка автозагрузки).
Ship with OS (Поставка вместе с операционной системой)	Показывает, была ли данная программа установлена в ходе установки операционной системы Windows.
Classification (Классификация)	Показывает, представляет ли программа угрозу конфиденциальным сведениям или безопасности компьютера.
Digitally Signed By (Автор цифровой подписи)	Имеет ли программное обеспечение цифровую подпись, если да, то принадлежит ли эта подпись производителю, указанному в списке. Если нет, то не рекомендуется доверять сведениям о производителе, предоставляемым с программным обеспечением, и следует просмотреть дополнительную информацию, прежде чем признать данное программное обеспечение надежным.

7.6. **Лабораторная работа.** Установка и использование Защитника Windows.

В этой лабораторной работе вы установите Защитника Windows, проверите дату последнего обновления, проведете проверку компьютера и обнаружите подозрительные действия.

Упражнение 1. Подготовительные действия

Вы скопируете потенциально нежелательное программное обеспечение Home Key Logger (клавиатурный шпион) на свой компьютер и создадите командный файл с подозрительными действиями (он регистрирует себя в реестре для автоматического запуска при каждом старте операционной системы).

1. Зарегистрируйтесь в системе как пользователь с правами администратора.
2. Скопируйте на рабочий стол архив с программой Home Key Logger (http://www.spvarsenal.com/cqi-bin/load.pl7familv-kevloqqer--webroot--otherproducts282)
3. С помощью проводника в корневой папке диска C: создайте папку «Test».
4. Выполните «Пуск» - «Выполнить» - «cmd».
5. Для создания командного файла c:\test\risk.bat, в командной строке выполните следующие действия:

```
c:
cd \test
copy con risk.bat
{Ctrl+Z}{Enter}
Exit
```

6. С помощью проводника откройте папку `C:\Test`. На файле `risk.bat` нажмите правую кнопку мыши. В появившемся контекстном меню выберите команду «Изменить».
7. После открытия Блокнота, наберите следующую команду (в одну строку):

```
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v
risk.bat /t REG SZ /d "C:\Test\risk.bat"
```

8. Сохраните изменения (команда меню «Файл | Сохранить») и закройте Блокнот.

7.6.2. Упражнение 2. Установка Защитника Windows

Вы выполните установку Защитника Windows на свой компьютер.

1. Зарегистрируйтесь в системе как пользователь с правами администратора и подключитесь к Интернету (если это ещё не сделано).
2. С помощью Internet Explorer откройте «Домашнюю страницу Защитника Windows» (http://www.microsoft.com/rus/athome/security/spyware/software/default.ms px) и щелкните по надписи «Загрузить здесь».
3. При появлении на странице надписи «Validation Required», щелкните кнопку «Continue».
4. При появлении в Internet Explorer панели информации со значком ***Щ*** о необходимости установки элемента управления ActiveX «Windows Genuine Advantage», щелкните левой кнопкой мыши по этой панели и выберите команду «Установить элемент управления ActiveX...».
5. При появлении предупреждения системы безопасности об установке ActiveX компонента, нажмите кнопку «Установить».
6. После успешной проверки лицензии Вашей ОС, выберите язык интерфейса Защитника Windows с помощью параметра «Change Language» и нажмите кнопку «Download» рядом с надписью «Genuine Microsoft Software». Примечание: Дальнейшие шаги предполагают, что Вы выбрали английский язык интерфейса.
7. После появления предупреждения системы безопасности, нажмите кнопку «Сохранить» (рис. 7.8) и выберите место для сохранения файла `WindowsDefender.msi`. Если во время установки Защитника Windows возникнут ошибки, вы всегда сможете запустить установку повторно, если сохраните установщик на диск.
8. Запустите файл `WindowsDefender.msi`. Если после запуска вы увидите окно приветствия Мастера установки, то перейдите к пункту 11. Если вы увидите сообщение об отсутствии Windows Installer 3.1, то перейдите к пункту 9. Если вы увидите сообщение о необходимости обновления службы Windows Update, то перейдите к пункту 10.
9. Установите приложение Windows Installer 3.1. Для этого посетите сайт http://go.microsoft.com/fwlink/?LinkId=63848 описывающий требования к установке Защитника Windows. Как указывается на этой странице, посетите Центр загрузки Microsoft, чтобы установить Windows Installer. Для этого перейдите по ссылке «Microsoft Download Center» и следуйте инструкциям по загрузке и установке Windows Installer. Если необходимо, перезагрузите компьютер и вернитесь к п.8.
10. Обновите на Вашем компьютере службу Windows Update. Для этого воспользуйтесь либо внутренним сервером обновлений в Вашей орга

низации (если он существует), либо в Internet Explorer выполните команду меню «Сервис | Windows Update». Следуйте инструкциям на экране для обновления службы Windows Update. Если необходимо, перезагрузите компьютер и вернитесь к п.8.

11. После появления на экране окна приветствия Мастера установки, нажмите кнопку «Next». Прочтите лицензионное соглашение и если Вы его принимаете, то выберите «I accept the terms in the license agreement» и нажмите кнопку «Next».
12. На следующей странице выберите вариант «Use recommended settings» и нажмите кнопку «Next».
13. На следующей странице выберите вариант полной установки «Com- plete» и нажмите кнопку «Next».
14. При появлении сообщения о готовности к установке Защитника Windows, нажмите кнопку «Install».
15. После успешной установки, отключите параметр «Check for updated definitions and run a quick scan now» и нажмите кнопку «Finish».

7.6.3. Упражнение 3. Обновление определений Защитника Windows

Вы выполните обновление определений Защитника Windows.

1. Зарегистрируйтесь в системе как пользователь с правами администратора и подключитесь к Интернету (если это ещё не сделано).
2. Запустите Защитник Windows (Пуск - Все программы - Windows Defender).
3. В разделе «Status» проверьте версию установленных обновлений и дату их создания (Параметр «Definition version:»).

4. Щелкните по треугольнику **(В)** рядом со знаком помощи (^Ep). В появившемся списке выберите команду «About Windows Defender». В появившемся окне нажмите кнопку «Check for Updates».
5. Дождитесь появления сообщения «Windows Defender is up-to-date with definitions and engine upgrades».
6. На главной странице (возникает по нажатию кнопки «Home») проверьте версию установленных обновлений и дату их создания.

7.6.4. Упражнение 4. Быстрое сканирование компьютера

Вы выполните быструю проверку Вашего компьютера с помощью Защитника Windows и удалите обнаруженное нежелательное ПО.

1. Зарегистрируйтесь в системе как пользователь с правами администратора.
2. Запустите Защитник Windows (Пуск - Все программы - Windows Defender).
3. Щелкните по треугольнику (Э) рядом с надписью «Scan». В появившемся списке выберите команду «Quick Scan».

4. После окончания сканирования, при появлении раздела «Review potentially unwanted items», щелкните ПО надписи В Review items detected ***by*** scanning..
5. На странице «Scan Results» просмотрите все обнаруженные объекты и для каждого выберите желаемое действие.
6. Посмотрите расположение обнаруженного объекта «Home Key Logger» (раздел «Resources:»). Для этого объекта выберите действие «Remove» и нажмите внизу кнопку «Apply Actions».
7. После появления в столбце «Status» сообщения «Succeeded», проверьте, что объект действительно удален с диска.

7.6.5. Упражнение 5. Обнаружение подозрительных действий

Вы включите получение уведомлений обо всех подозрительных событиях и посмотрите реагирование Защитника Windows на некоторые из них.

1. Зарегистрируйтесь в системе как пользователь с правами администратора.
2. Для того чтобы получать уведомления обо всех подозрительных действиях, совершаемых на Вашем компьютере, необходимо в разделе «Choose if Windows Defender should notify you about:» включить параметр «Software that has not yet been classified for risks». Для этого на странице «Tools» выберите раздел «Options» и там включите указанный выше параметр.
3. Запустите редактор реестра для контроля происходящих действий. Для этого выполните «Пуск» - «Выполнить» - «regedit». Откройте ключ «Мой компьютер\HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVer sion\Run».
4. С помощью Проводника запустите на выполнение командный файл «C:\Test\risk.bat».
5. При появлении в области уведомлений (правый нижний угол экрана) сообщения «Windows Defender detected changes», щелкните по нему левой кнопкой мыши.
6. В открывшемся окне Защитника Windows, просмотрите описание обнаруженного события.
7. С помощью редактора реестра, проверьте появление значения «risk.bat».
8. В столбце «Action», выберите действие «Block» и нажмите кнопку «Ap- ply Actions».
9. После отображения статуса «Succeeded», проверьте в редакторе реестра, что значение «risk.bat» действительно удалено (если необходимо, выполните команду «Вид | Обновить» в редакторе реестра).
10. Закройте все открытые окна.

7.7. Закрепление материала

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

1. Дайте определение термину «шпионская» программа.

2. Перечислите действия, которые могут выполнять программы-шпионы.

3. Перечислите вероятные признаки наличия на компьютере «шпионского» либо нежелательного ПО.

4. Перечислите технологий Microsoft обеспечивающие защиту компьютеров от программ-шпионов и других нежелательных программ.

5. Перечислите технологий Microsoft обеспечивающие защиту компьютеров от вирусов и вредоносного ПО.

6. Что такое сообщество Microsoft SpyNet?

7. Какие функции выполняет обозреватель программ (Software Explorer) входящий в состав Защитника Windows?

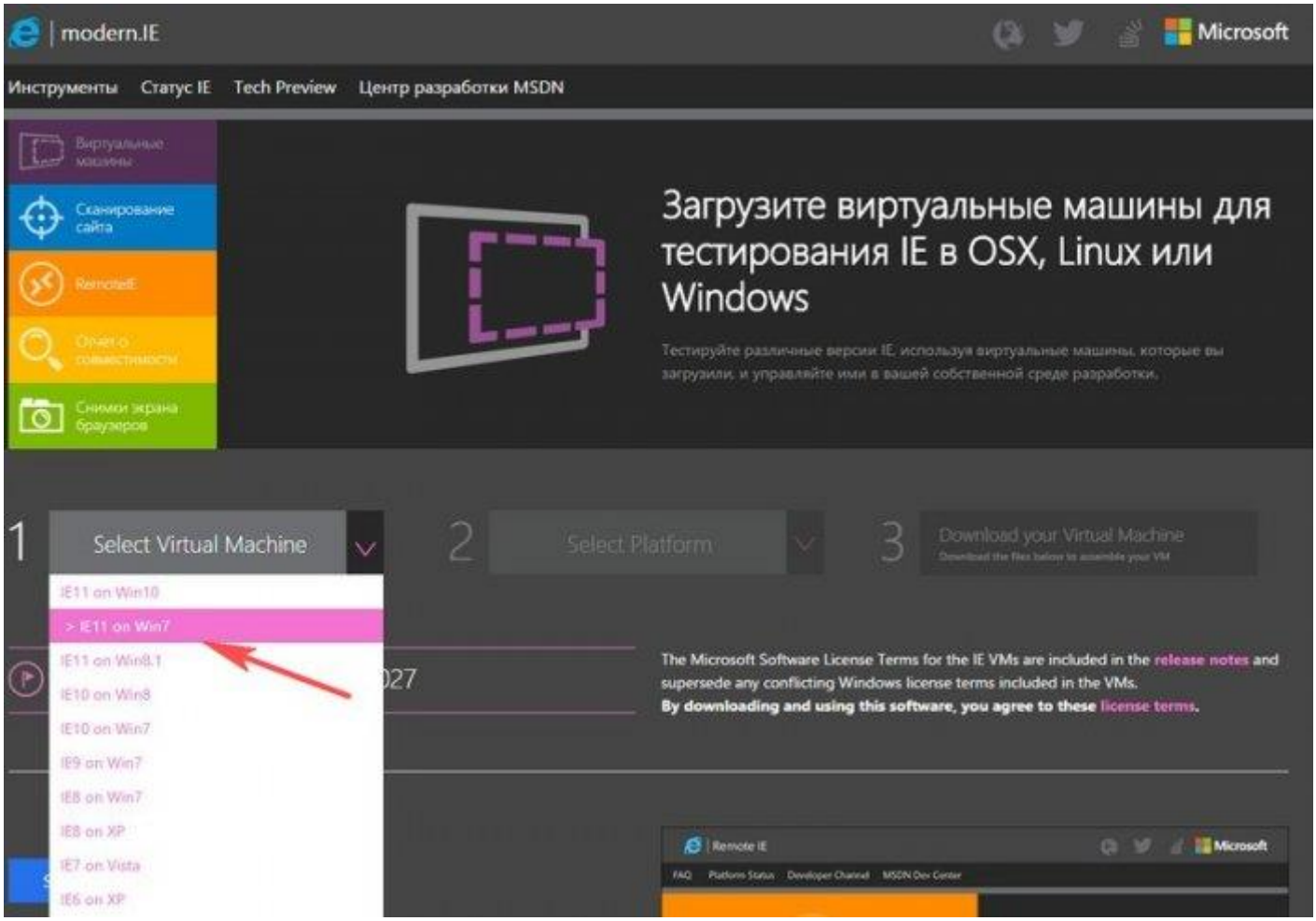
Тема: Установка и использование виртуальной машины.

Как скачать готовую виртуальную машину с Windows 7

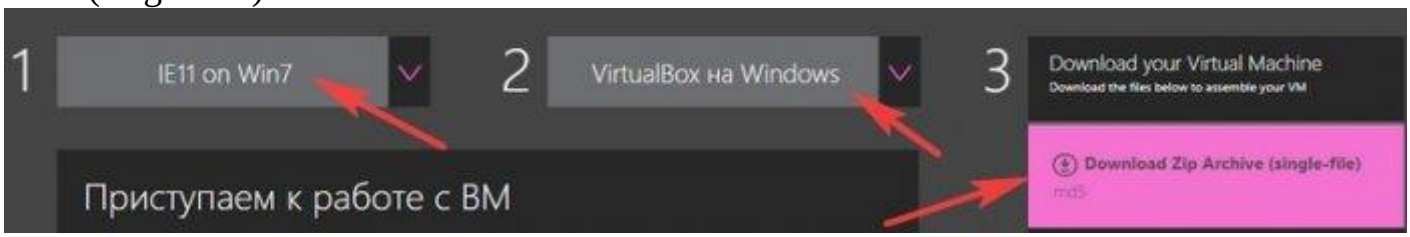
В первую очередь устананавливаем себе на компьютер виртуальную машину VirtualBox, затем скачиваем файл готовой виртуальной машины с Windows 7.

Примечание: На нашем сайте есть статьи о VirtualBox, которые Вам могут пригодится
1. Как установить на виртуальную машину операционные системы Windows 7 и Windows 8
2. Как скачать готовую виртуальную машину с Windows 8.1
3. Как установить Windows 10 на виртуальную машину
4. Как загрузить виртуальную машину VirtualBox с USB-флешки
5. Как создать в VirtualBox общую папку соединяющую виртуальную машину и действующую операционную систему
6. Как в VirtualBox подключить флешку

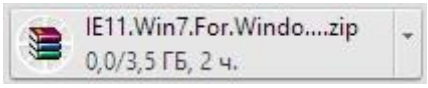
Переходим по ссылке на сайт — modern.ie, на нём можно скачать готовые виртуальные машины с Windows XP, Vista, 7, 8, 8.1, 10.
на английском:
https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
Выбираем Windows 7.



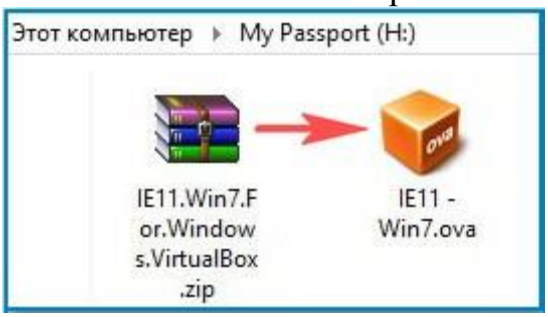
Затем выбираем версию виртуальной машины VirtualBox и жмём на кнопку Download Zip Archive (single-file)



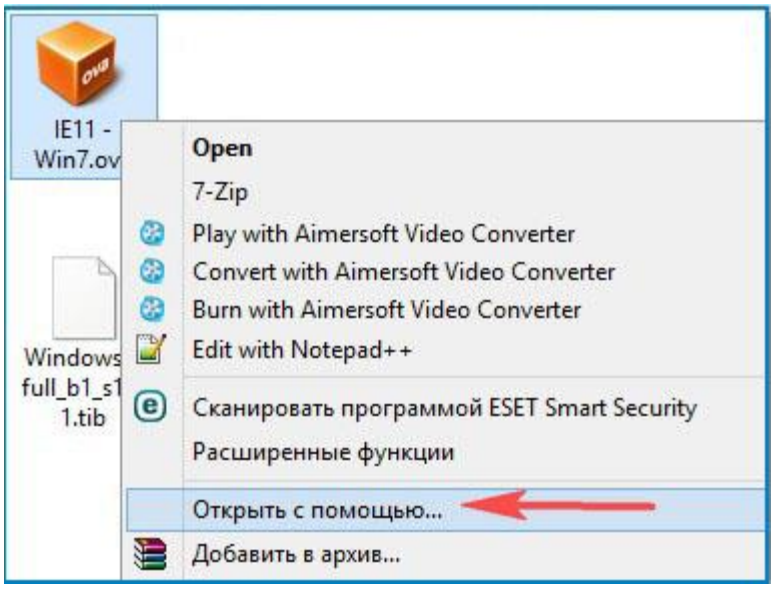
и файл готовой виртуальной машины с Windows 7 скачивается нам на компьютер в архиве.



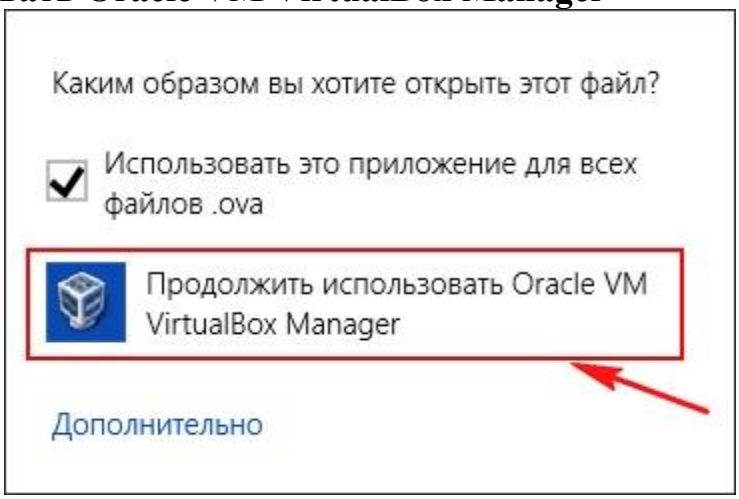
Извлекаем файл виртуальной машины Windows 7 из архива.



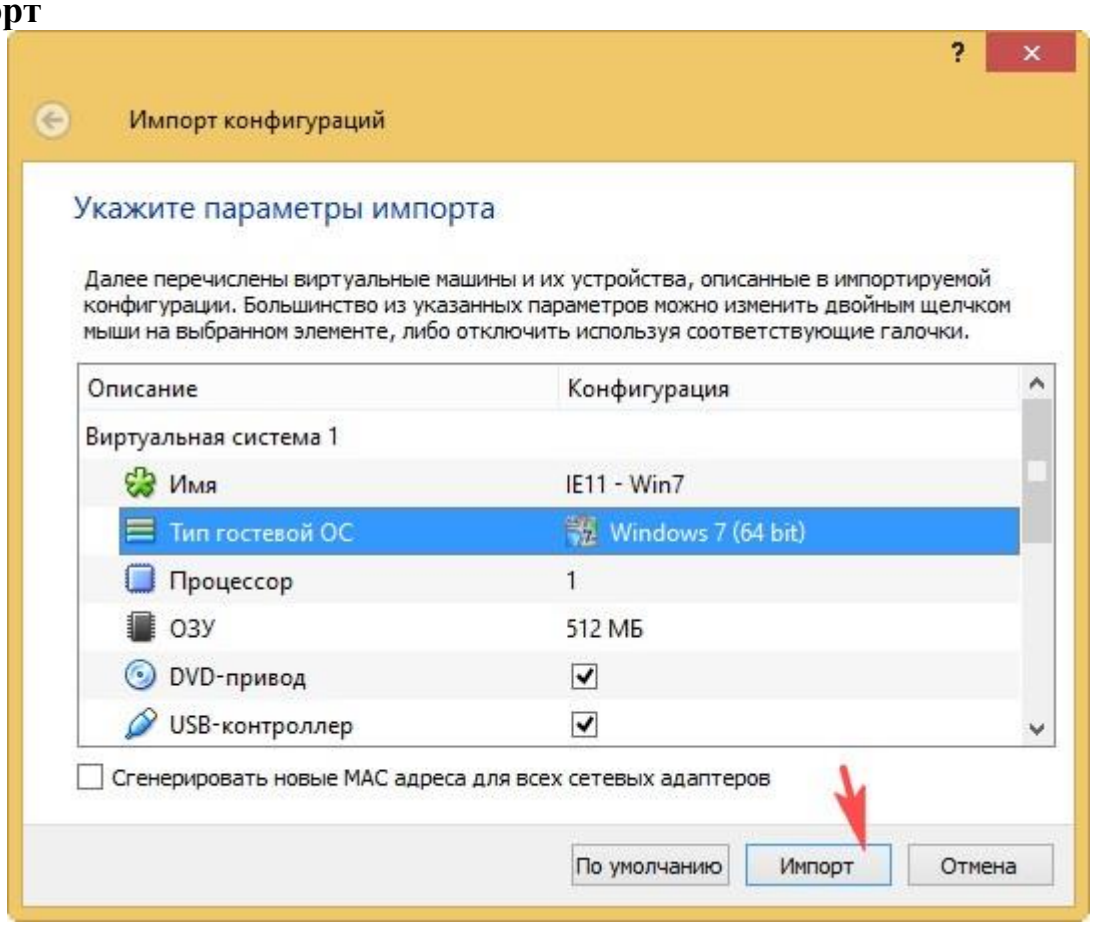
Щёлкаем на нём правой мышью и выбираем **Открыть с помощью**



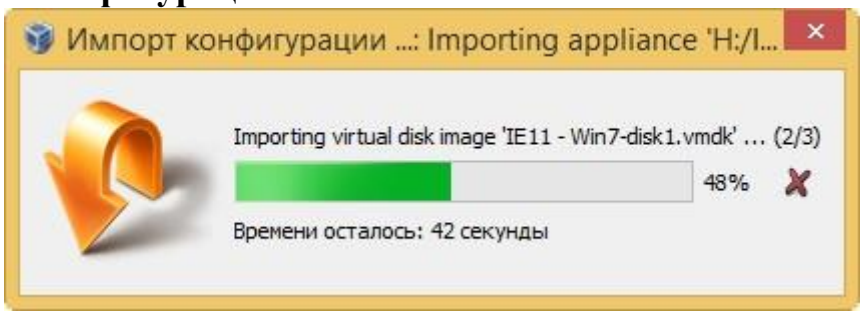
Продолжить использовать Oracle VM VirtualBox Manager



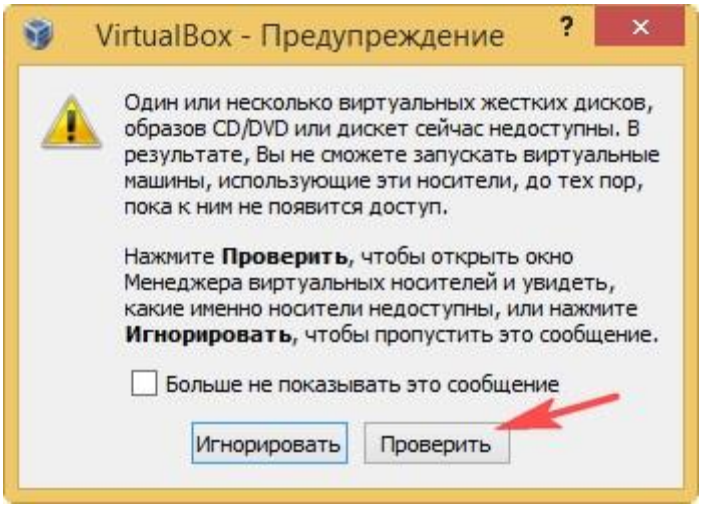
Указываем параметры импорта будущей виртуальной машины. Можно ничего не менять. Жмём **Импорт**



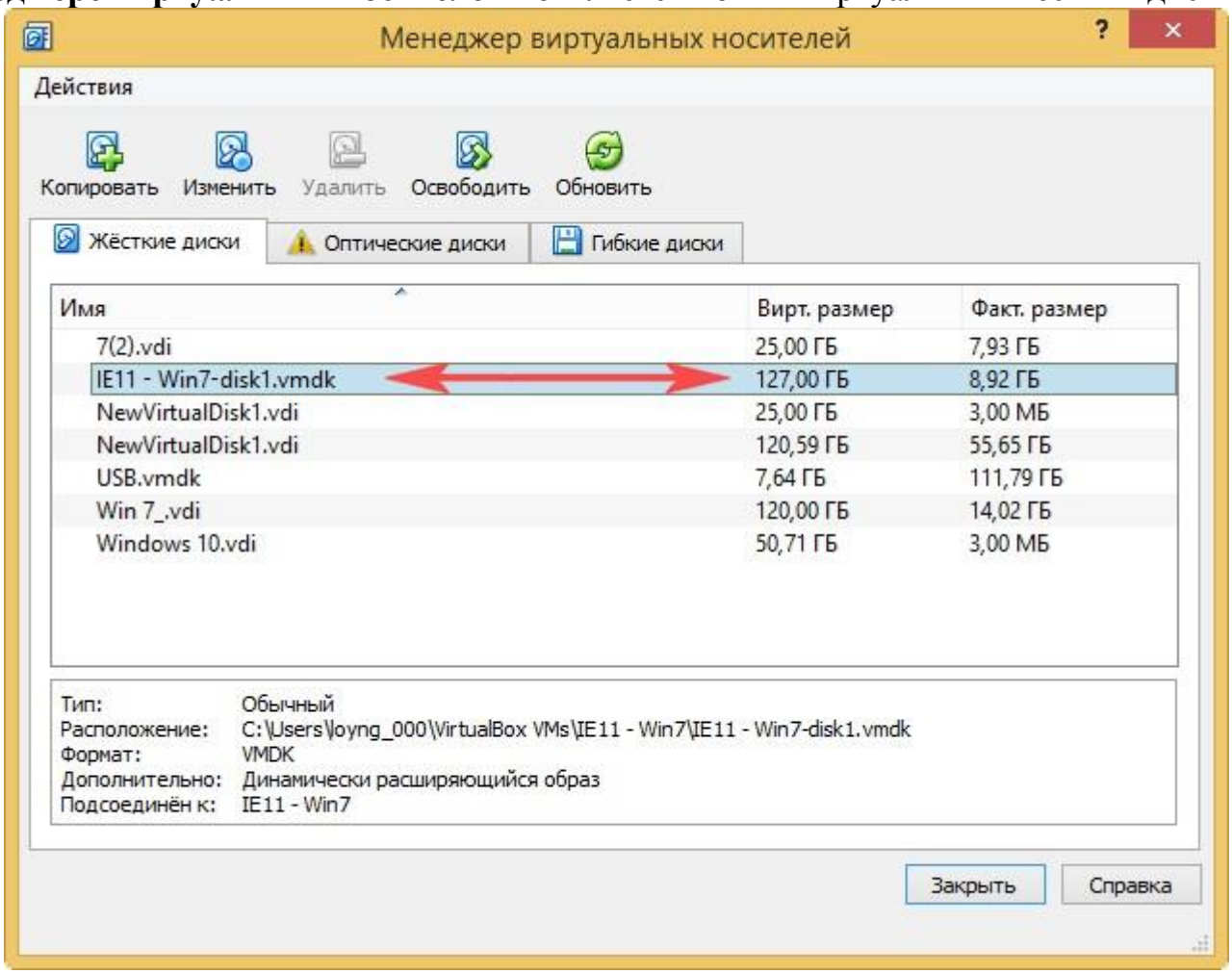
Происходит **Импорт конфигурации**



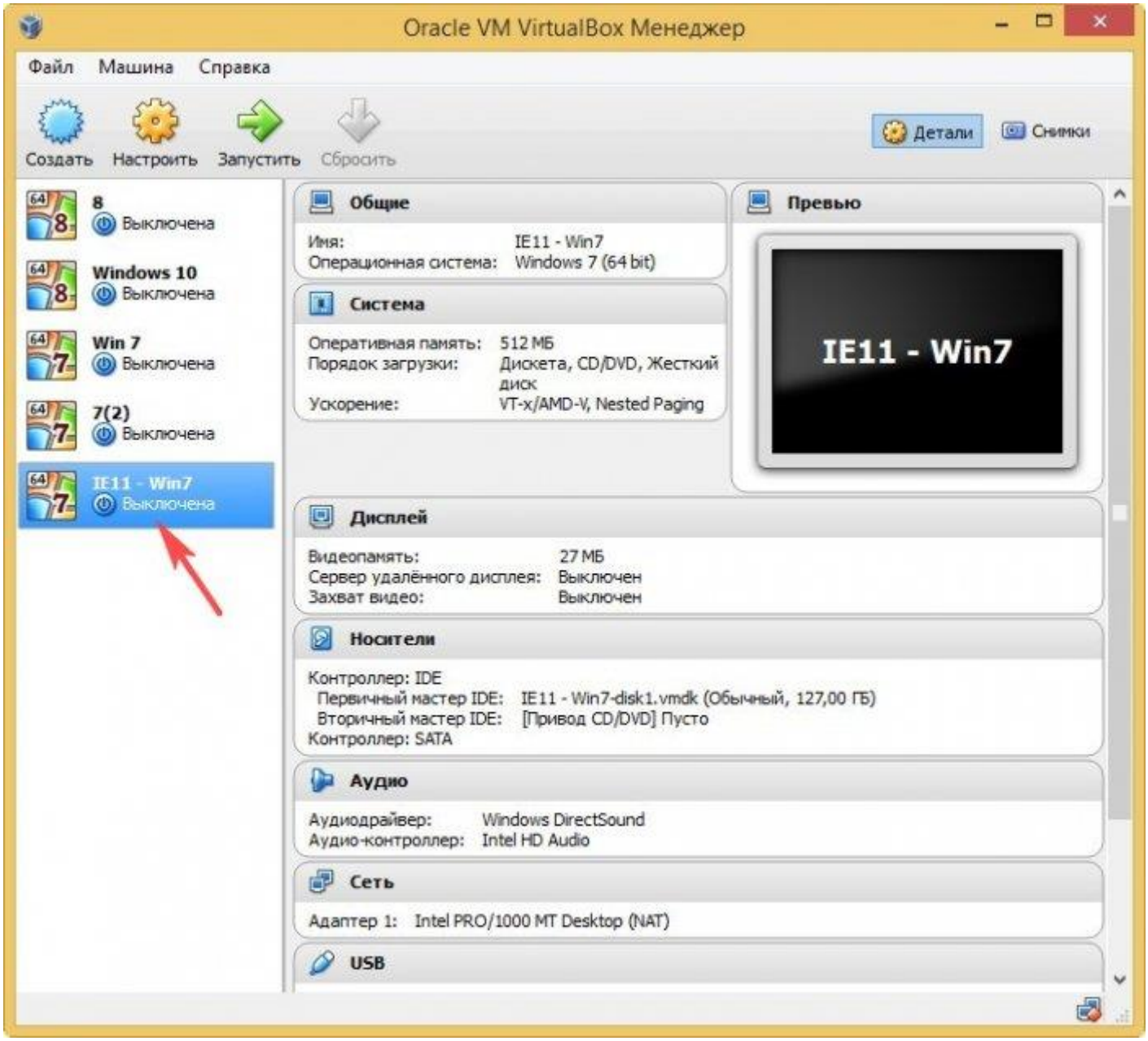
Проверить



В менеджере виртуальных носителей появляется новый виртуальный жёсткий диск

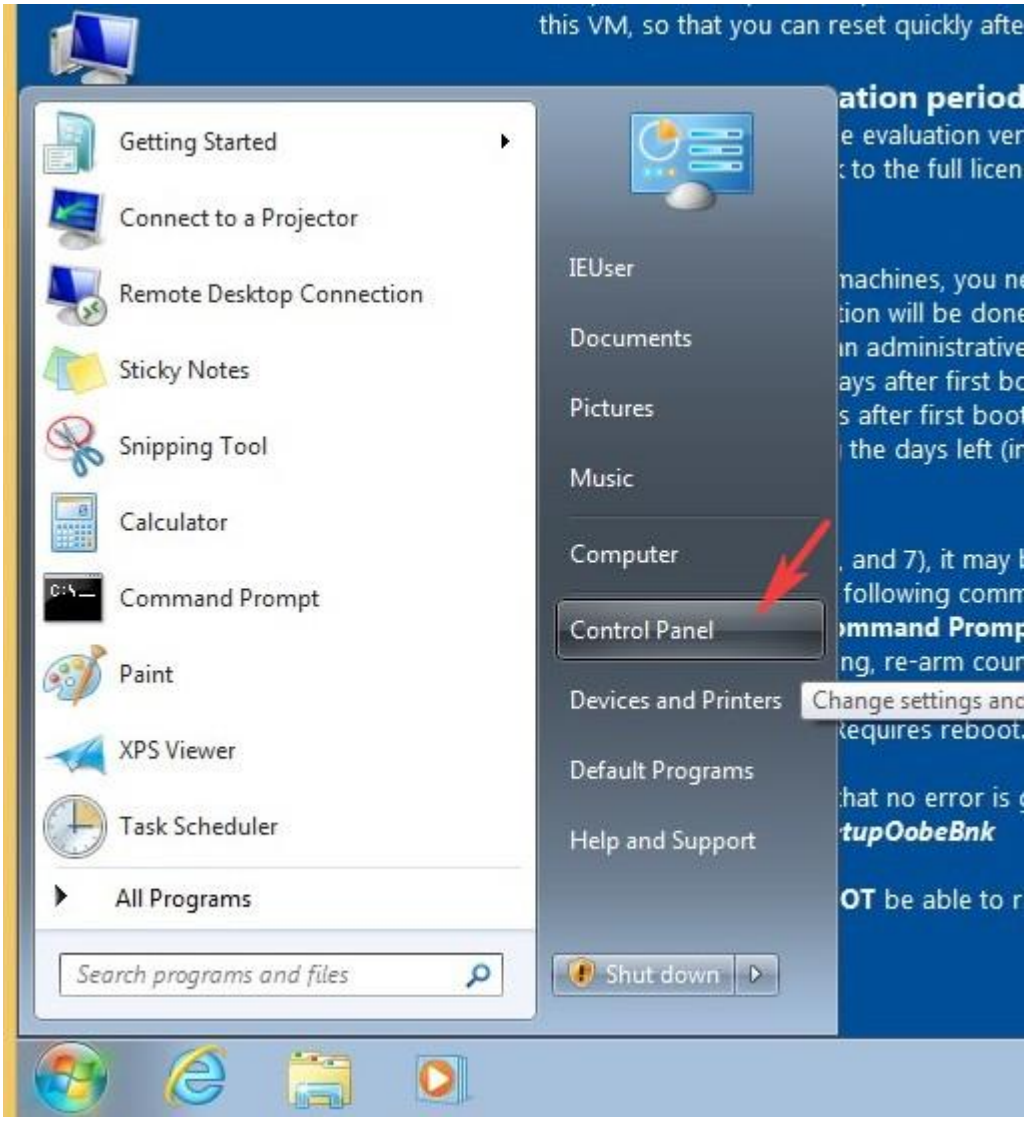


Запускаем новую виртуальную машину

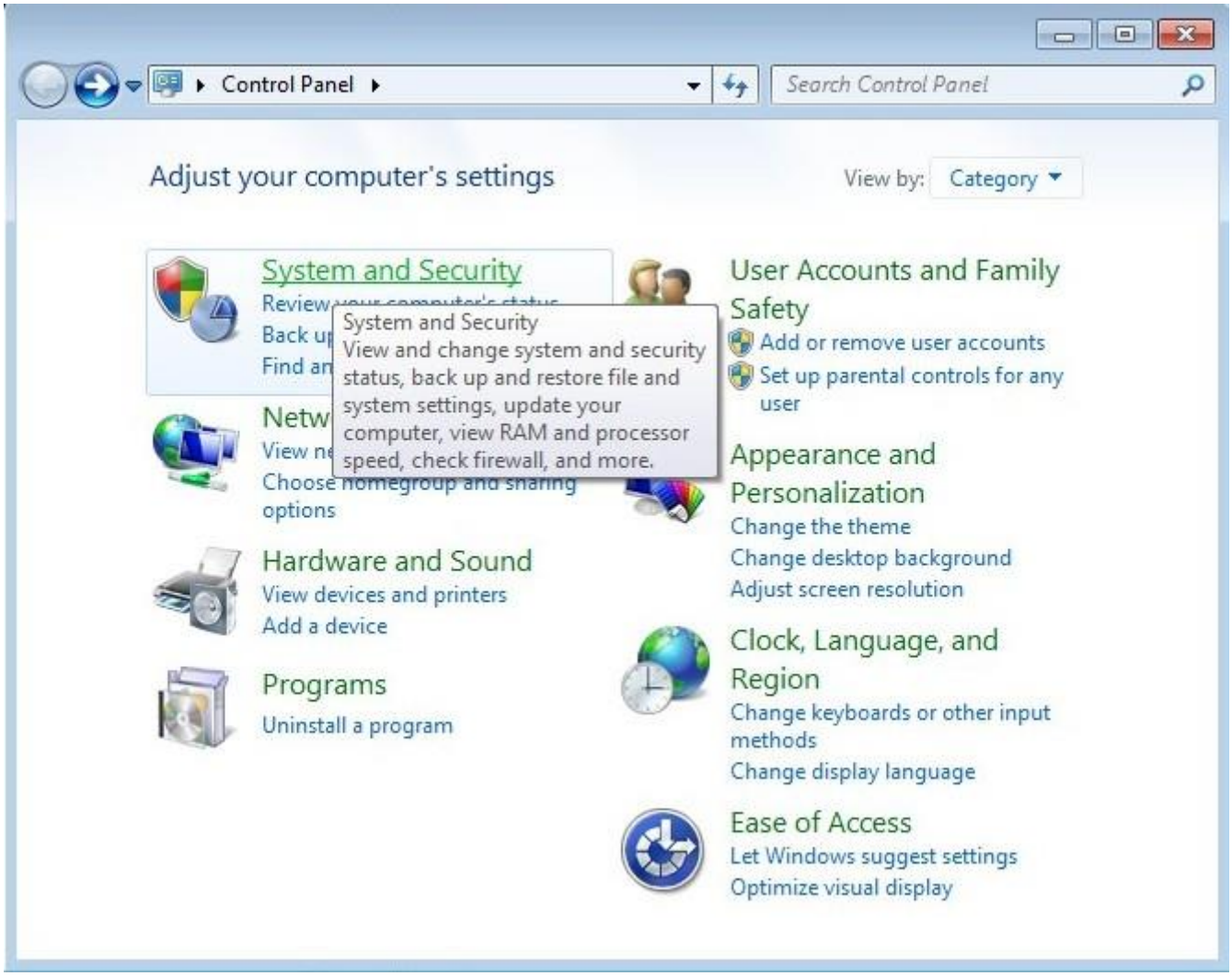


Запускается Windows 7 на английском языке, который мы запросто можем сменить на русский. Во первых Вы можете русифицировать Windows 7 по этой статье, а во вторых сменить интерфейс Windows 7 можно с помощью Центра обновления Windows. Такой способ я Вам ни разу не показывал, так что смотрите, пригодится.

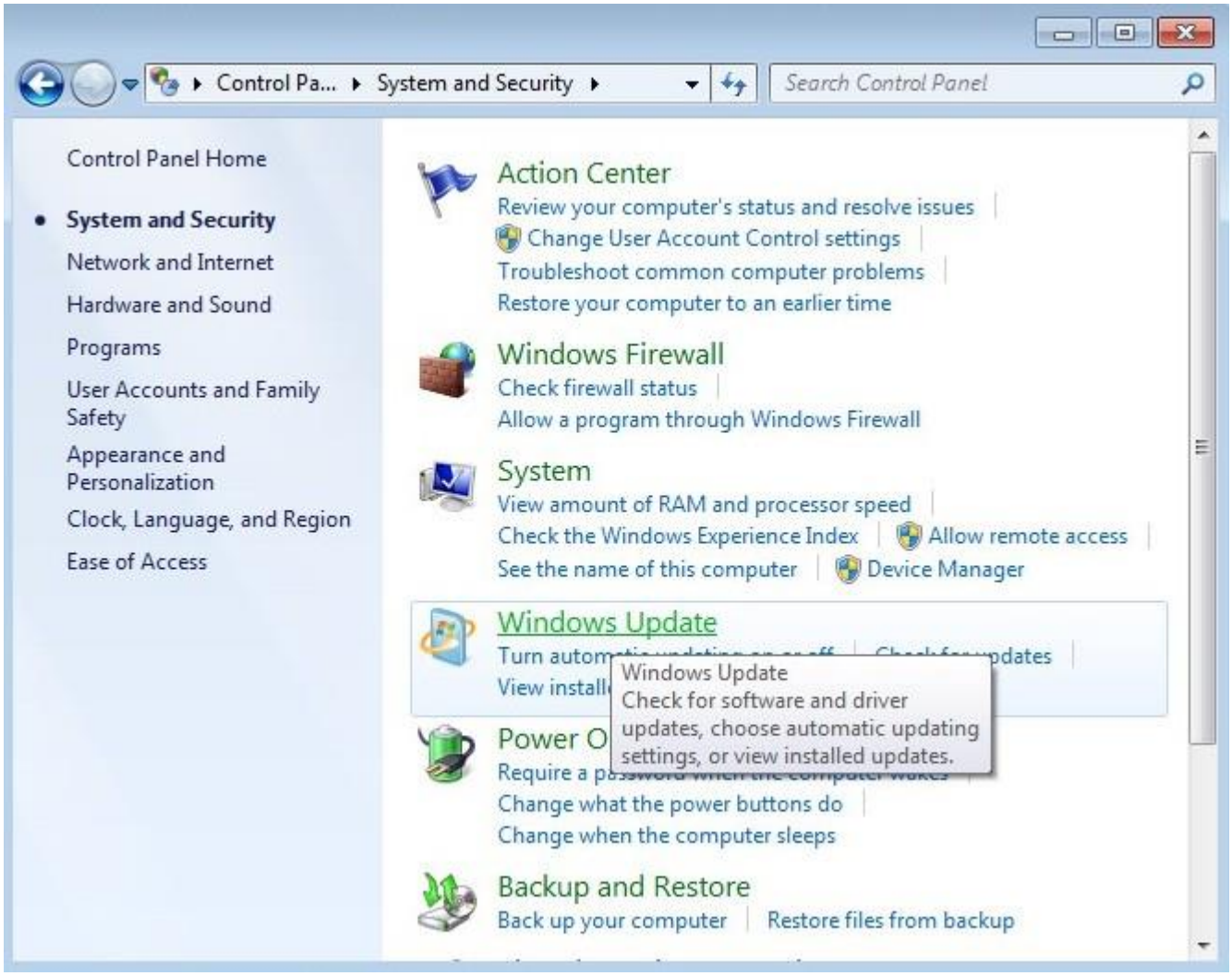
Щёлкаем на меню **Пуск** левой мышью и выбираем **Control Panel**



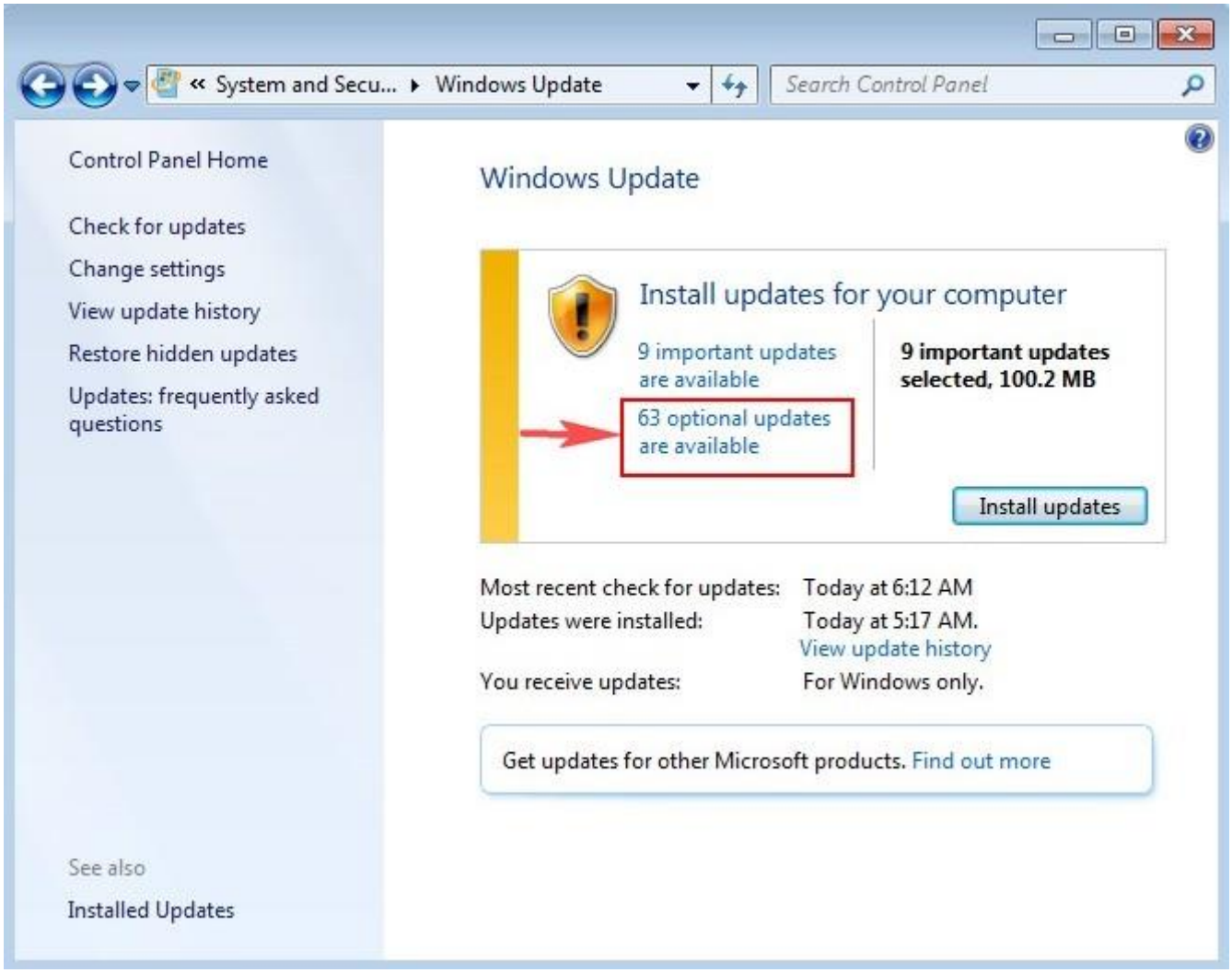
System and Security



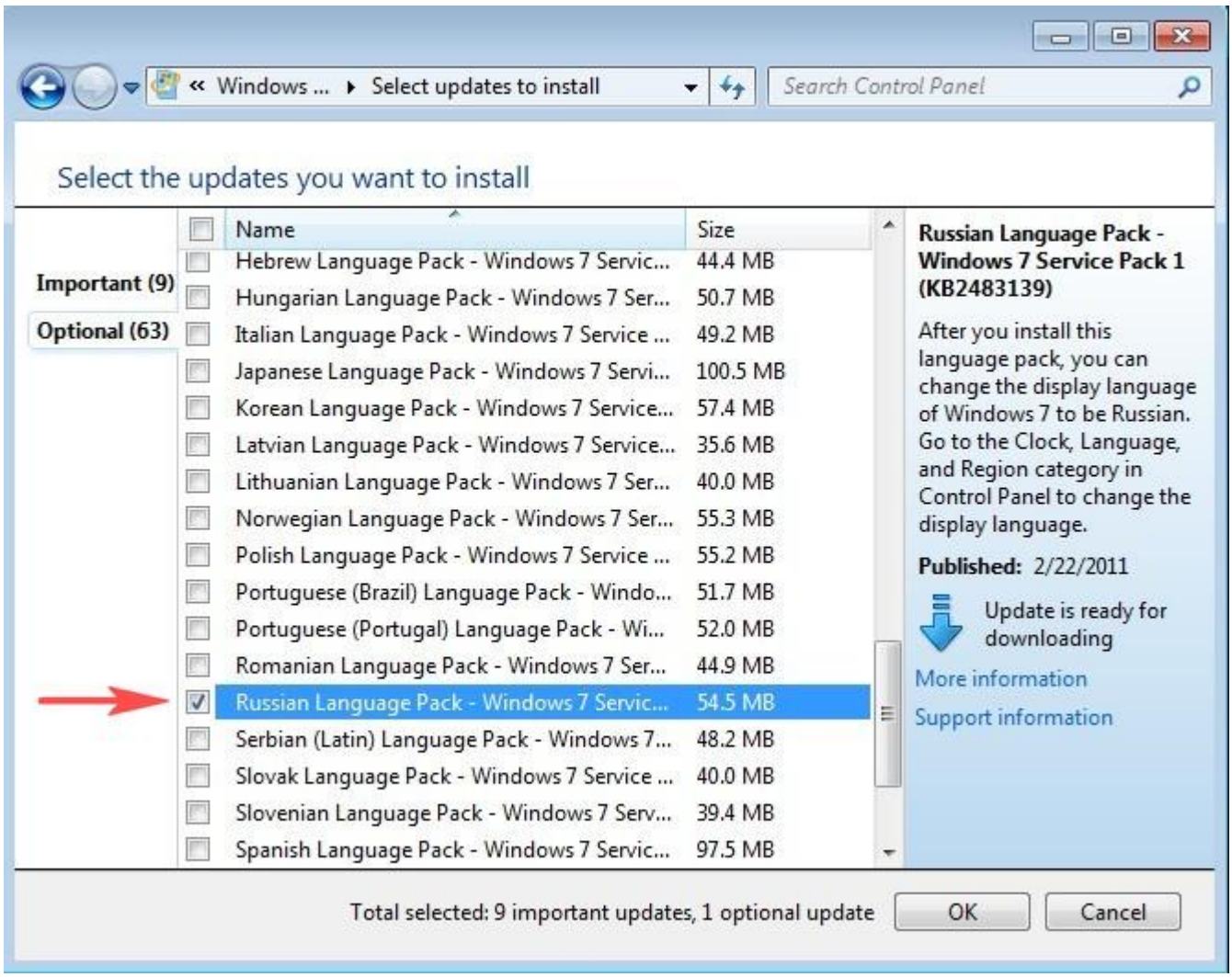
Windows Update



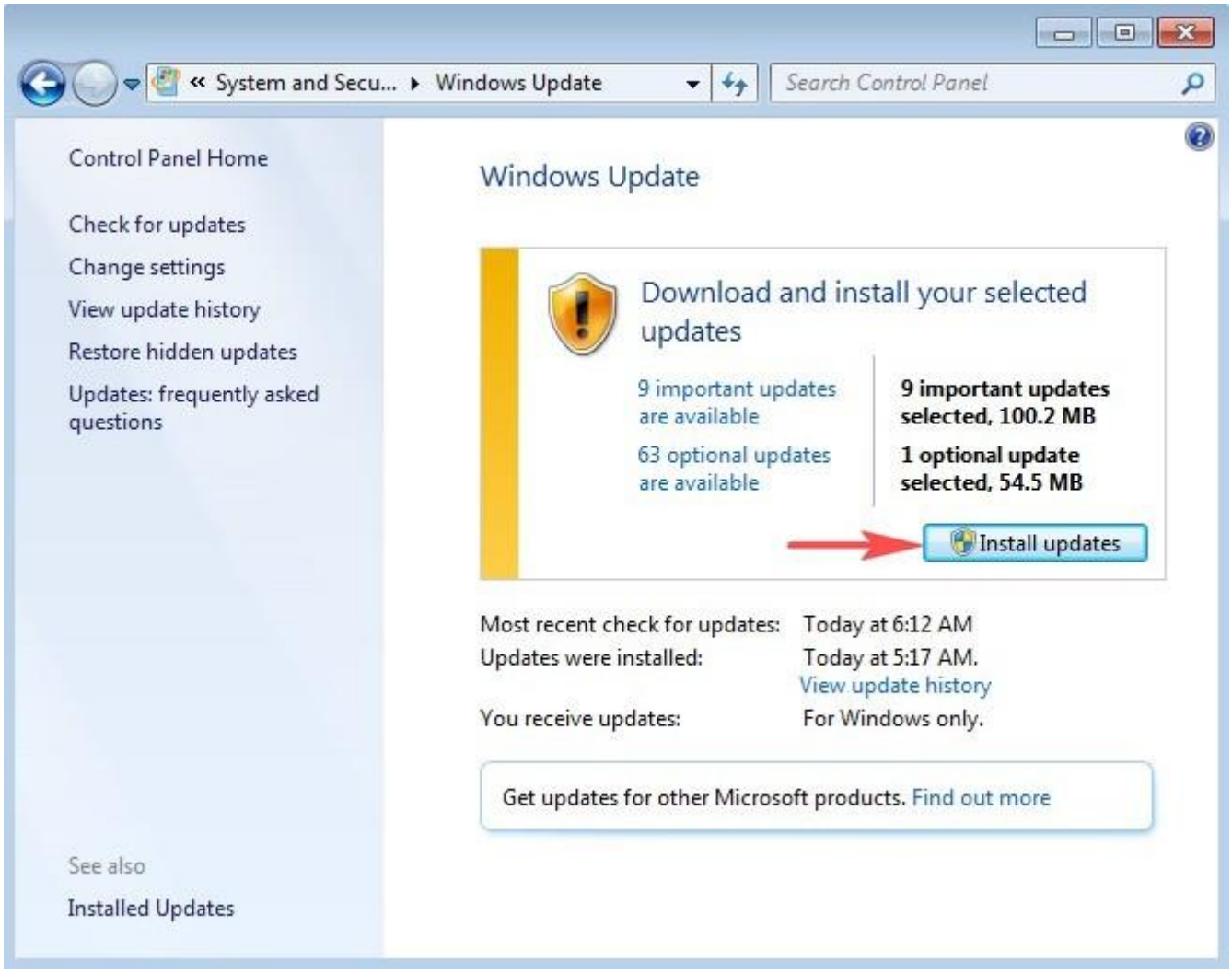
Щёлкните по надписи **Необязательные обновления** (Optional updates)

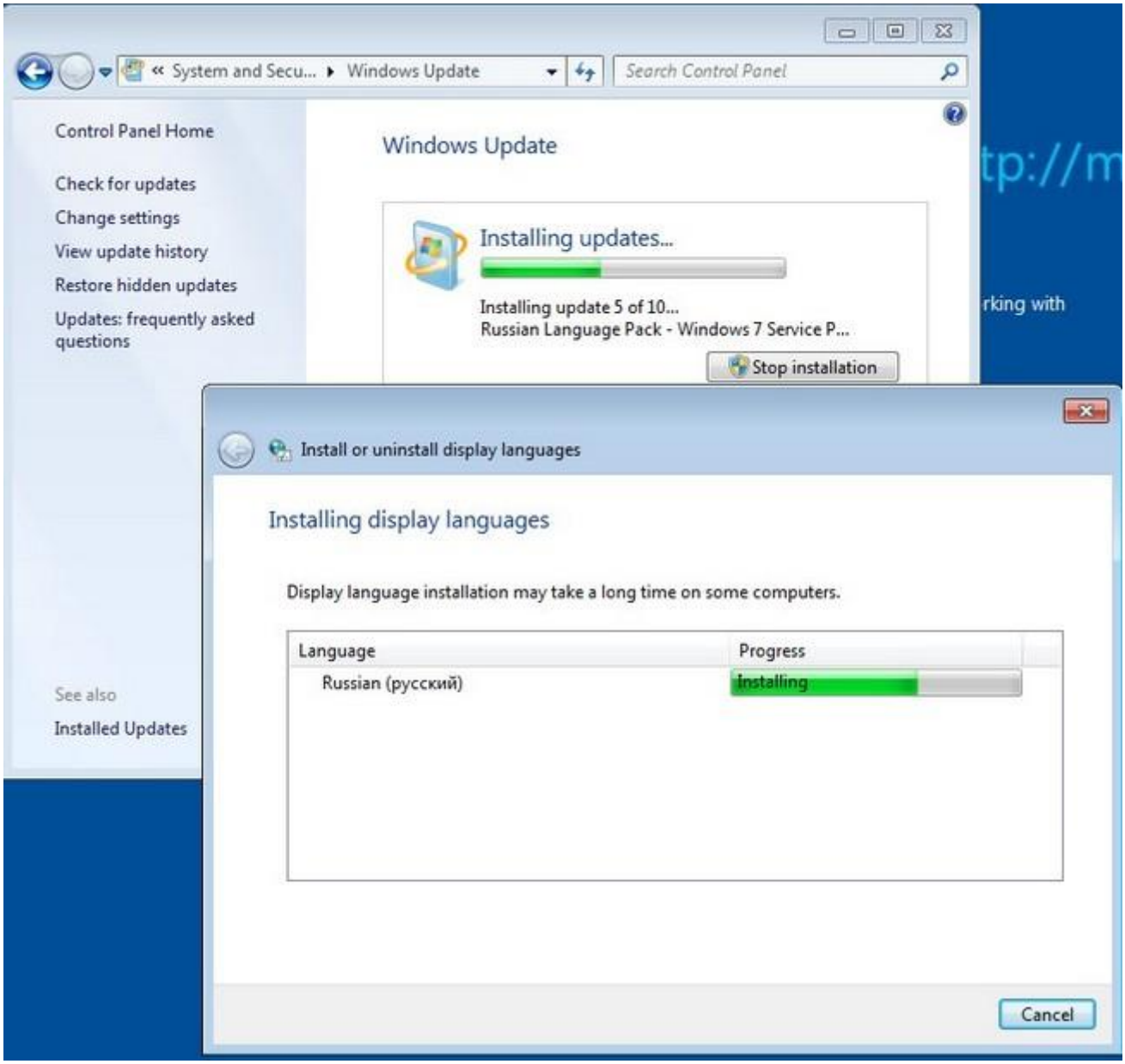


Возникает список **Windows Languages Packs**. Отмечаем галочкой **Русский язык** и жмём **ОК**

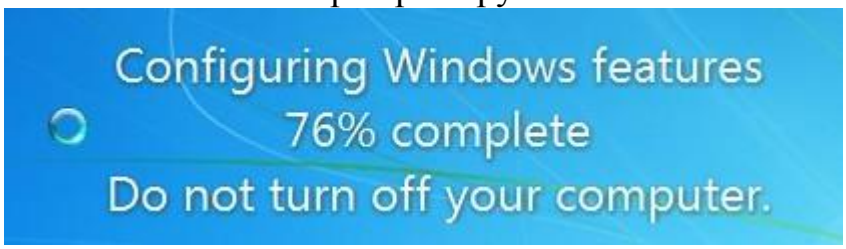


Нажмём кнопку **Install updates** (Начать установку) и Windows загрузит, а затем установит выбранный язык.

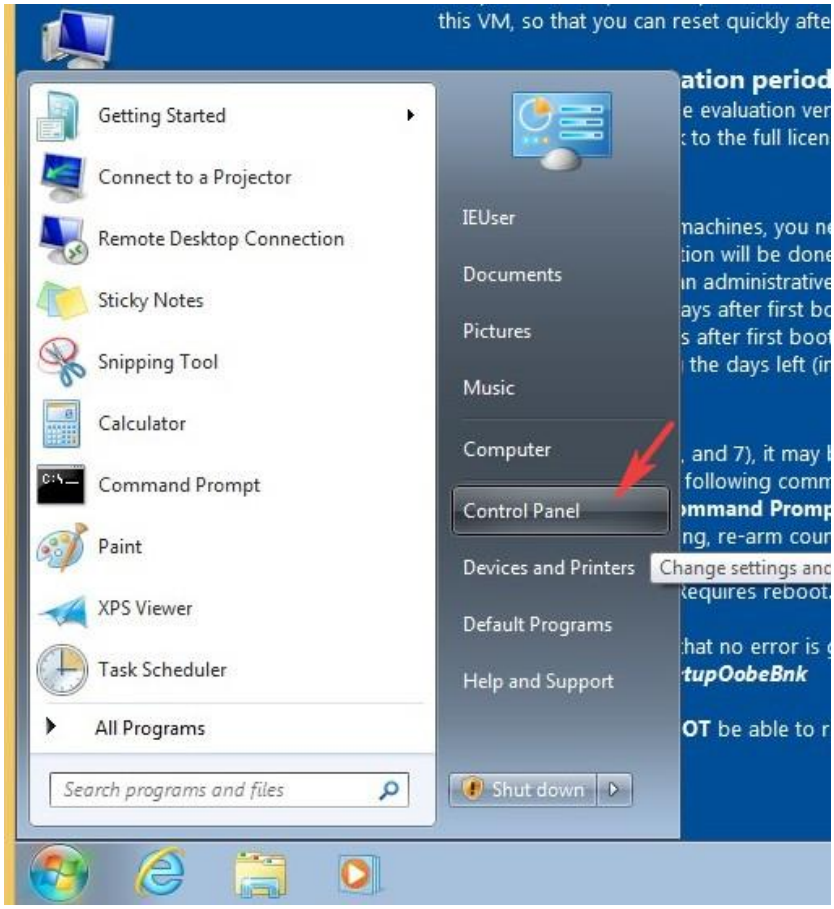

« System and Secu... ▸ Windows Update
Search Control Panel
Control Panel Home
Check for updates
Change settings
View update history
Restore hidden updates
Updates: frequently asked questions
See also
Installed Updates
Windows Update
Download and install your selected updates
9 important updates are available
63 optional updates are available
9 important updates selected, 100.2 MB
1 optional update selected, 54.5 MB
Install updates
Most recent check for updates: Today at 6:12 AM
Updates were installed: Today at 5:17 AM.
View update history
You receive updates: For Windows only.
Get updates for other Microsoft products. Find out more



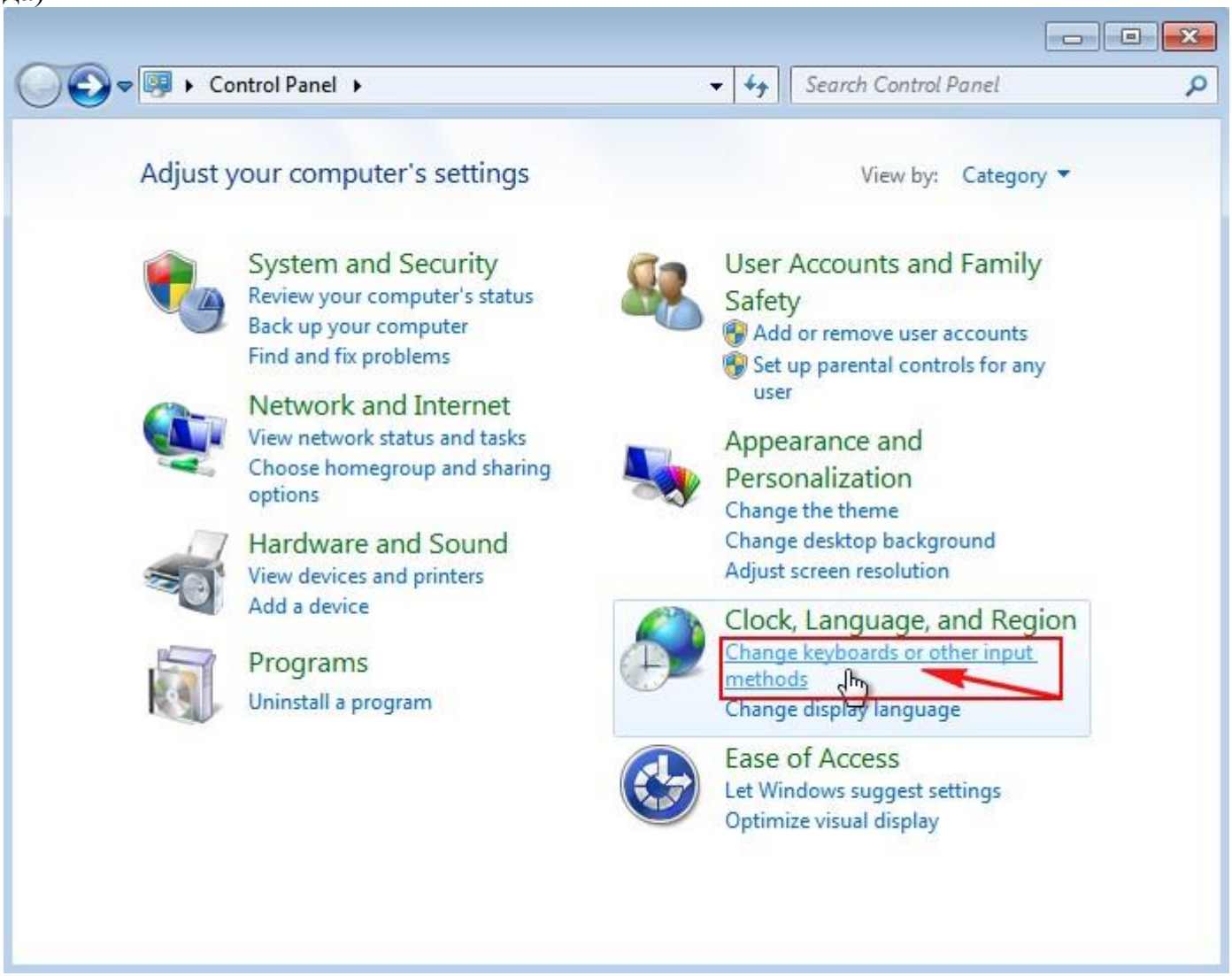
После скачивания обновлений компьютер перезагружается



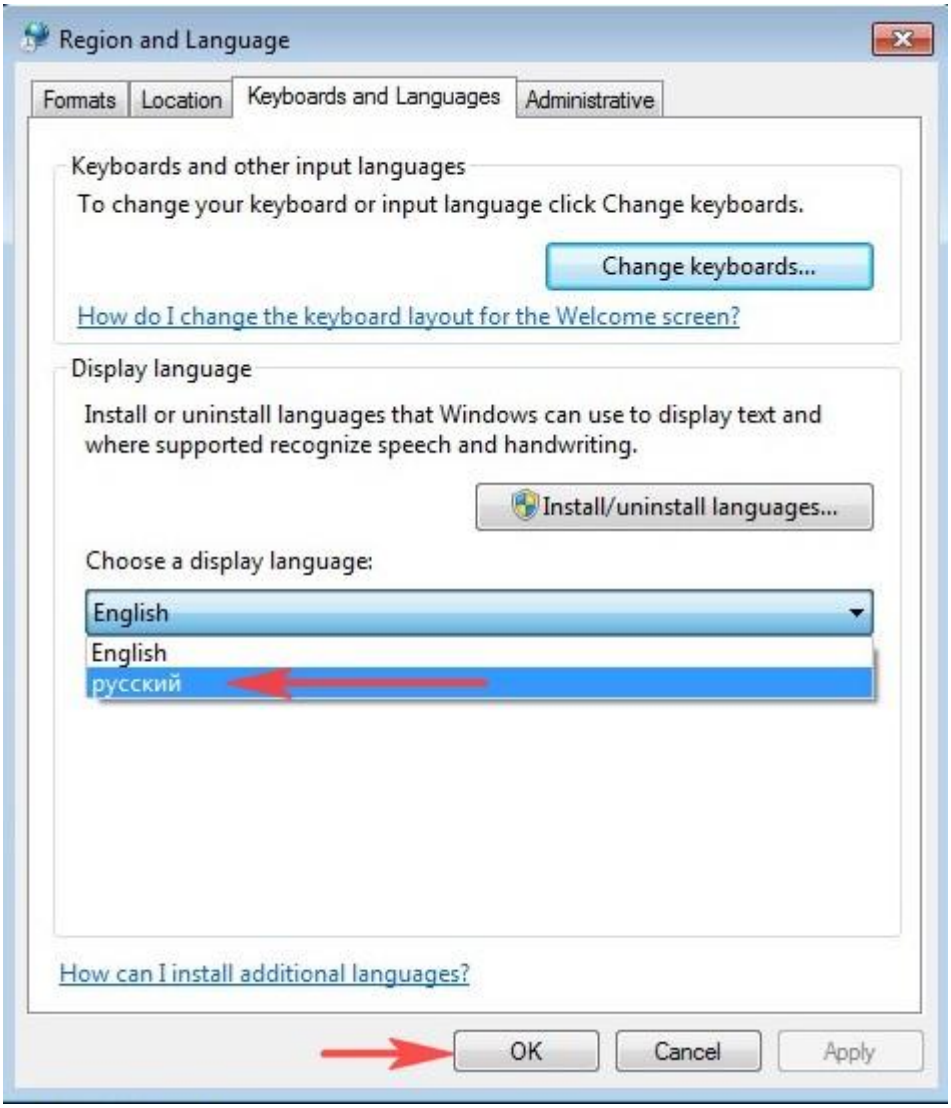
После перезагрузки опять щёлкаем левой мышью на меню **Пуск** и выбираем **Control Panel**

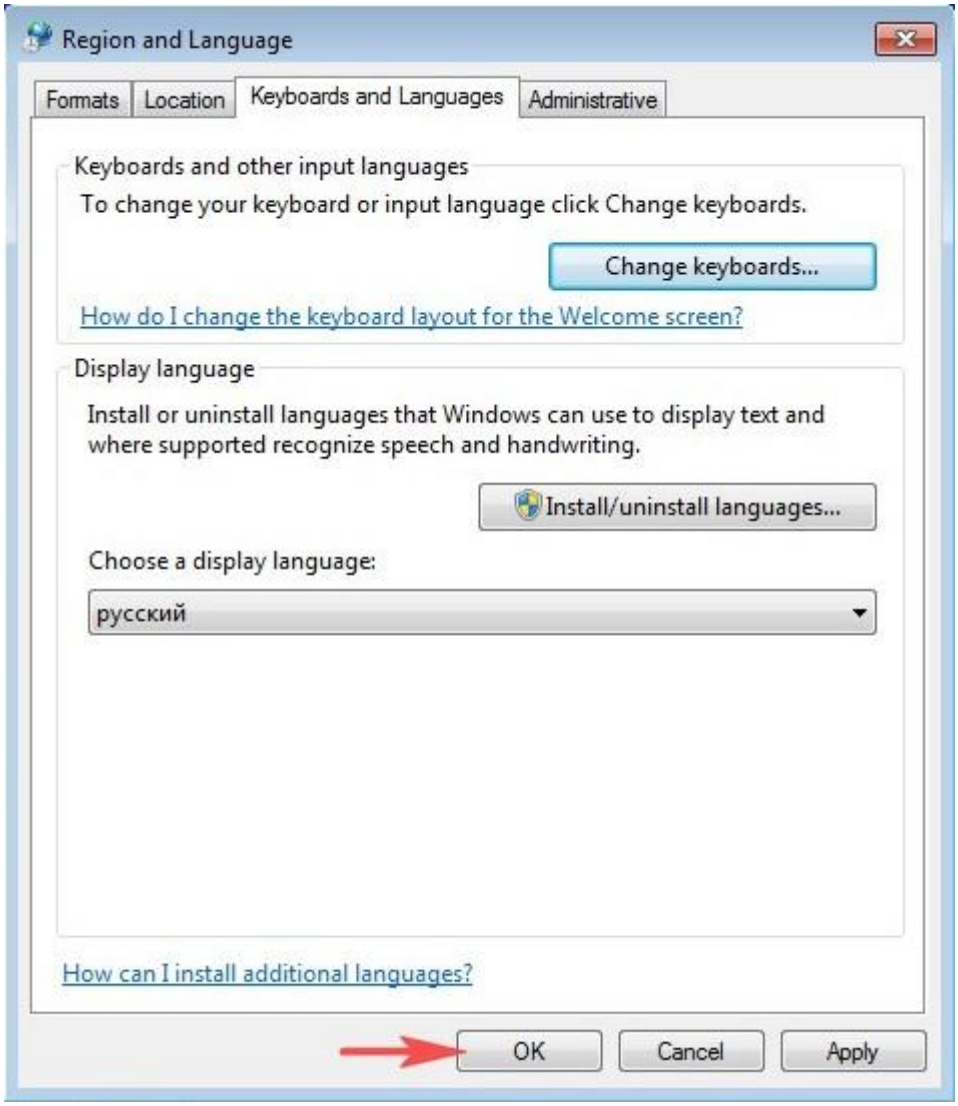


Change keyboards or other input methods (Смена раскладки клавиатуры или других способов ввода)

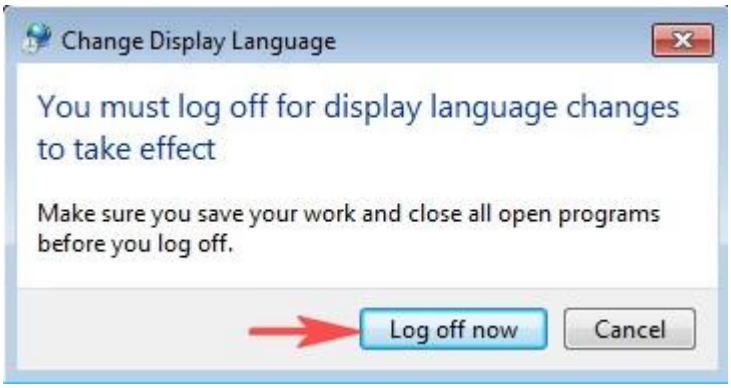


Выбираем **Русский язык** и жмём **ОК**.





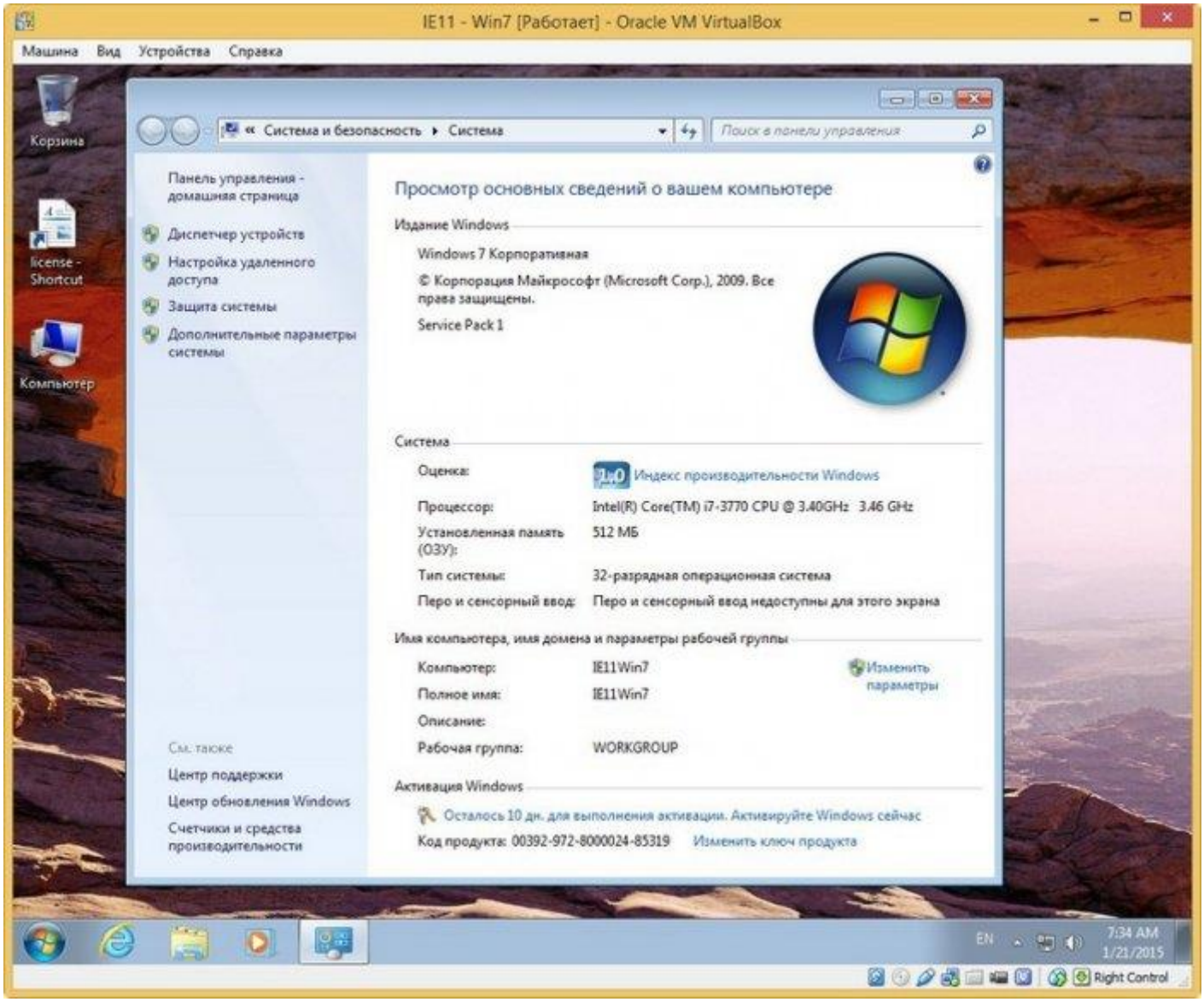
Log off now



Вводим пароль **Passw0rd!**

0 это цифра.

Windows 7 русифицирована.


IE11 - Win7 [Работает] - Oracle VM VirtualBox
Машина Вид Устройства Справка
Корзина
license - Shortcut
Компьютер
« Система и безопасность ▸ Система
Поиск в панели управления
Панель управления - домашняя страница
Диспетчер устройств
Настройка удаленного доступа
Защита системы
Дополнительные параметры системы
Просмотр основных сведений о вашем компьютере
Издание Windows
Windows 7 Корпоративная
© Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
Service Pack 1
Система
Оценка:
Индекс производительности Windows
Процессор:
Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz 3.46 GHz
Установленная память (ОЗУ):
512 МБ
Тип системы:
32-разрядная операционная система
Перо и сенсорный ввод:
Перо и сенсорный ввод недоступны для этого экрана
Имя компьютера, имя домена и параметры рабочей группы
Компьютер:
IE11Win7
Изменить параметры
Полное имя:
IE11Win7
Описание:
Рабочая группа:
WORKGROUP
Активация Windows
Осталось 10 дн. для выполнения активации. Активируйте Windows сейчас
Код продукта: 00392-972-8000024-85319
Изменить ключ продукта
См. также
Центр поддержки
Центр обновления Windows
Счетчики и средства производительности
EN
7:34 AM
1/21/2015
Right Control

Тема: Механизмы развертывания сетевой инфраструктуры на основе ОС Windows

СОДЕРЖАНИЕ

2. Механизмы развертывания сетевой инфраструктуры на основе ОС Windows 2003/XP

В данном пособии далее будем рассматривать компьютерную сеть, серверы которой управляются операционными системами Windows Server 2003, а рабочие станции - Windows XP (SP2), другими словами, сетевую инфраструктуру на основе ОС Windows 2003/XP.

На этом занятии рассмотрим способы развертывания такой сетевой инфраструктуры. Термин «развертывание» *(англ.* deployment) не следует путать с «установкой» *(англ.* install) операционных систем. Развертывание подразумевает автоматизацию процесса установки ОС на компьютер. Возможны механизмы развертывания операционных систем Microsoft, когда этот процесс становится полностью автоматическим.

Почему важно уметь обеспечивать быстрое развертывание сетевой инфраструктуры? Любая компьютерная система организации не застрахована от серьезных аварий, вызванных естественными причинами (действиями злоумышленников, халатностью или некомпетентностью сотрудников). В то же время, у каждой организации есть функции, которые руководство считает критически важными, и они должны выполняться несмотря ни на что [6]. Сетевая инфраструктура, для большинства современных организаций, является базисом для выполнения бизнес-процессов. Поэтому очень важно уметь восстанавливать (разворачивать) сетевую инфраструктуру в короткие сроки и с минимальными затратами.

Рассмотрим на этом занятии два основных механизма развертывания, которые применяются для ОС Microsoft:

- Метод дублирования дисков с использованием утилиты *Sysprep*;
- Метод удаленной установки с использованием *сервера удаленной установки (RIS)*.

На практике очень редко прибегают к автоматической установке серверной ОС. Для небольших и средних организаций наиболее важной задачей может являться развертывание ОС для рабочих станций с необходимым прикладным ПО. Поэтому на лабораторных работах рассмотрим указанные выше методы на примере ОС Windows XP Professional.

Прежде всего

Для изучения материалов этой главы необходимы следующие ресурсы:

- Компьютер под управлением операционной системы Windows XP Professional с параметрами по умолчанию, объемом оперативной памяти не менее 1 Гб и сетевой картой.
- Свободное место на жестком диске не менее 6 Гб.
- Загрузочный компакт-диск с дистрибутивом Windows XP Professional.
- Загрузочный компакт-диск с дистрибутивом Windows Server 2003.

2.1. Метод дублирования дисков с использованием утилиты Sysprep

Идея метода заключается в том, что если необходимо установить ОС Windows XP Professional сразу на несколько компьютеров с одинаковой конфигурацией оборудования, то на одном из компьютеров создается образ диска, на который устанавливают ОС с необходимым прикладным ПО. Затем этот образ копируется на остальные компьютеры.

Преимущество метода над обычной установкой состоит, прежде всего, в экономии времени. Другой плюс заключается в том, что создав один раз образ диска, вы получаете базовую точку развертывания рабочего места пользователя, к которой всегда можно вернуться, если на каком-то из компьютеров возникнут проблемы.

Главную роль в реализации метода играет утилита «Подготовка системы» - Sysprep (System Preparation). Она предотвращает проблему, с которой можно столкнуться при копировании образа диска, связанную с уникальным кодом безопасности (SID, Security Identifier). Каждый компьютер в сети должен иметь уникальный код безопасности. Если просто копировать образ диска, то каждый конечный компьютер будет иметь тот же код безопасности, что и основной компьютер. Из-за конфликтов SID сеть не будет работать. Утилита Sysprep помогает решить эту проблему, удаляя уникальный код безопасности на основном компьютере перед копированием образа диска. При запуске копии системы на конечном компьютере Sysprep генерирует новый уникальный код безопасности.

Для использования утилиты Sysprep в процессе дублирования дисков должны выполняться следующие требования [9]:

- Основной и конечные компьютеры должны иметь совместимые файлы уровня аппаратных абстракций (HAL, Hardware Abstraction Layer);
- Контроллеры жестких дисков на основном и конечных компьютерах должны быть одинаковыми;
- Устройства Plug and Play, такие как модемы, звуковые карты, сетевые карты, видеокарты и т. д., могут быть различными. Тем не менее, все драйверы устройств, не включенные в файл Drivers.cab, должны быть перенесены в основной компьютер перед запуском Sysprep. Следует убедиться в том, что драйверы доступны на конечном компьютере при первом запуске, чтобы технология Plug and Play могла обнаружить и установить устройства;
- Объем жесткого диска на конечном компьютере должен быть не меньше объема жесткого диска на основном компьютере.
- Если версии BIOS (Basic Input-Output System, базовая система ввода вывода) на основном и конечных компьютерах различаются, рекомендуется предварительно протестировать процесс установки.

Далее рассмотрим основные шаги выполнения метода дублирования дисков с использованием утилиты Sysprep.

2.1.1. Шаг 1

Установите и настройте Windows XP Professional на тестовом компьютере (если необходимо, то установите драйверы оборудования, не включенные в файл Drivers.cab). Установите необходимое прикладное ПО (архиваторы, антивирусы, офисные пакеты и т.д.), включая пакеты обновлений.

2.1.2. Шаг 2

Создайте файл ответов Sysprep.inf для того чтобы процесс развертывания был автоматическим. Данный шаг не является обязательным. Если файл ответов не создавать, то после копирования образа диска на целевой компьютер при их последующем включении запустится мастер миниустановки (Mini-Setup Wizard), который будет запрашивать ввод различных параметров (пароль администратора, имя компьютера и т.д.).

Sysprep.inf - это текстовый файл, в котором записывается последовательность ответов, вводимых в диалоговых окнах графического интерфейса пользователя при установке Windows XP Professional. Для создания файла ответов Sysprep.inf, который потом будет использоваться утилитой Sysprep, можно воспользоваться любым текстовым редактором или диспетчером установки (см. п. 2.3.1).

Файл Sysprep.inf должен храниться в папке Sysprep в корневом каталоге диска, на котором установлена ОС Windows XP Professional, или на гибком диске. Программа установки не может использовать папки с другими названиями. Параметра для указания произвольного файла ответов для мастера мини-установки не существует.

2.1.3. Шаг 3

Запустите на тестовом компьютере утилиту Sysprep, файлы которой находятся в архиве \Support\Tools\Deploy.cab на установочном диске Windows XP Professional. На экране появится диалоговое окно «Программа подготовки системы 2.0» (см. рис. 2.1), предупреждающее, что запуск программы Sysprep может привести к изменению некоторых параметров безопасности. Нажав кнопку «ОК» утилита Sysprep продолжит работу.

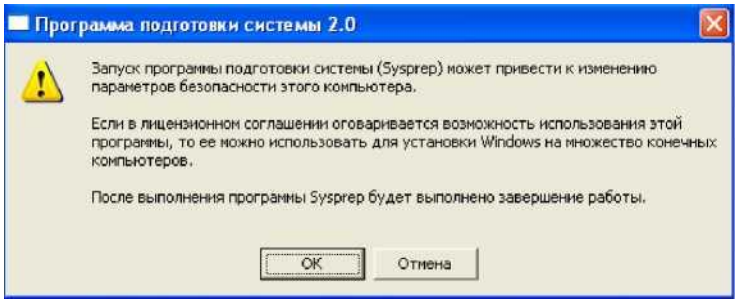


Рис. 2.1. Окно «Программа подготовки системы 2.0», появляющееся при запуске утилиты Sysprep.

В табл. 2.1. приведен состав и описание файлов утилиты Sysprep.

Таблица 2.1

Состав утилиты Sysprep

Файл	**Описание**
Sysprep.exe	Используется для запуска утилиты Sysprep.
Setupcl.exe	Необходимая компонента используется Sysprep.exe для создания SID.
Factory.exe	Вспомогательная программа, используемая вместе с Sysprep.exe для внесения изменений в стандартную конфигурацию перед переносом ее на целевые компьютеры (фабричный режим).
Sysprep.inf	Файл ответов (необязательный), который может быть использован для полной или частичной автоматизации установки.
Winbom.ini	Файл ответов (необязательный) для программы Factory.exe.

2.1.4. Шаг 4

Скопируйте образ диска на целевые компьютеры. Для этого потребуется специальное ПО для клонирования дисков, предоставляемые сторонними фирмами. Наиболее популярными являются утилиты Ghost фирмы Symantec, Drive Image Pro фирмы PowerQuest и др. [4] Все перечисленные утилиты работают примерно одинаково. Компьютер загружается в режиме DOS, потом запускается программа формирования образа диска. Можно получить образ всего диска или единственного раздела и сохранить его на другом разделе, диске или общем сетевом накопителе. Впоследствии сохраненный образ можно восстановить на другом диске. Жесткие диски не обязательно должны иметь одинаковую емкость, но загружаемый образ не должен быть больше целевого диска.

2.1.5. Шаг 5

Включите целевые компьютеры, после того как завершится копирование образа диска с тестового компьютера. Если утилита Sysprep обнаружила файл ответов Sysprep.inf, то появится окно «Установка Windows XP» (см. рис. 2.2) и через некоторое время загрузится ОС Windows XP Professional. В противном случае запустится мастер мини-установки.

Рис. 2.2. Окно «Установка Windows XP», появляющееся при развертывании образа диска утилитой Sysprep с использованием файла ответов.

Если приложение Sysprep.exe запускалось из папки %system-drive%\Sysprep, то после завершения установки Windows XP Professional эта папка и ее содержимое автоматически удаляются!

2.2. Метод удаленной установки

Наиболее эффективным методом развертывания ОС Windows XP Professional является удаленная установка. Ее можно проводить, если сетевая инфраструктура основана на ОС Windows Server 2003, а клиентские компьютеры поддерживают удаленную загрузку [1].

Удаленная установка (remote installation) - это процесс установки соединения с сервером, на котором запущена служба RIS (Remote Installation Services), и последующего запуска автоматической установки клиентской ОС, например Windows XP Professional, на целевой компьютер, подключенный к сети.

2.2.1. Предварительные требования для проведения метода

Для выполнения удаленной установки клиентский компьютер должен иметь BIOS и сетевой адаптер, поддерживающие технологию предзагрузочной среды выполнения - PXE (Pre-boot execution Environment). Технология PXE используется для установки соединения с сервером RIS. Убедитесь, что на всех клиентских компьютерах в BIOS имеется возможность установить в качестве загрузочного устройства сетевой адаптер. Если такая возможность отсутствует, то необходимо создать загрузочную дискету удаленной установки при помощи утилиты «Генератор дисков удаленной загрузки» - rbfg.exe (Remote Boot Disc Generator). Файл rbfg.exe располо

жен в папке \RemoteInstall\Admin\i386 на сервере удаленной установки RIS.

Для функционирования сервера RIS в сетевой инфраструктуре необходимо наличие следующих сетевых служб [9]:

- Служба DNS требуется для поиска в сети серверов RIS. Клиент RIS запрашивает у сервера DNS имя и IP-адрес сервера RIS.
- Служба DHCP. Для установки сетевого соединения клиент RIS должен иметь IP-адрес. Но так как на клиентском компьютере еще нет операционной системы, назначить статический IP-адрес невозможно, поэтому необходимо использовать динамическую адресацию. Для этого в сети должен работать сервер DHCP.
- Служба Active Directory. RIS использует групповую политику Active Directory для определения разрешений учетных записей пользователей и компьютеров. Учетной записи пользователя, которая будет использоваться для проведения удаленной установки, должно быть назначено право «Вход в качестве пакетного задания» (Log On as a Batch Job) и разрешение на создание учетных записей в домене. Прежде чем сервер RIS сможет обслуживать запросы клиентских компьютеров, он должен быть авторизован в Active Directory. Также Active Directory используется для того, чтобы определить, какой сервер RIS должен использоваться для удаленной установки, если таких серверов в сети несколько.

Перечисленные сетевые службы не обязательно должны быть установлены на том же сервере, что и RIS, но они должны быть доступны в сетевой инфраструктуре.

Метод удаленной установки требует, чтобы RIS был установлен на том, к которому разрешен общий доступ через сеть. Общий том должен отвечать следующим требованиям [1]:

- Общий том не является тем же самым диском, с которого запускается Windows Server 2003;
- На общем томе имеется достаточно свободного места для хранения программного обеспечения RIS и различных образов Windows XP Professional;
- Общий том отформатирован с использованием файловой системы NTFS версии 5 или выше.

2.2.2. Установка и настройка RIS

Развертывание сервера удаленной установки в вашей сетевой инфраструктуре выполняется в два этапа:

- установка RIS-сервера;
- настройка RIS-сервера.

При установке ОС Windows Server 2003 на сервер служба RIS по умолчанию не устанавливается. С помощью компонента панели управления

«Установка и удаление программ» в разделе «Установка компонентов Windows» необходимо добавить «Службы удаленной установки». После этого в разделе «Администрирование» появляется компонент «Установка служб удаленной установки», позволяющий запустить мастер подготовки сервера RIS. При первом запуске мастера установки служб удаленной установки, выбирается диск для размещения RIS, папка для хранения установочных файлов, создается образ для удаленной установки клиентской ОС. После завершения процесса установки службы RIS появится окно, представленное на рис. 2.3.

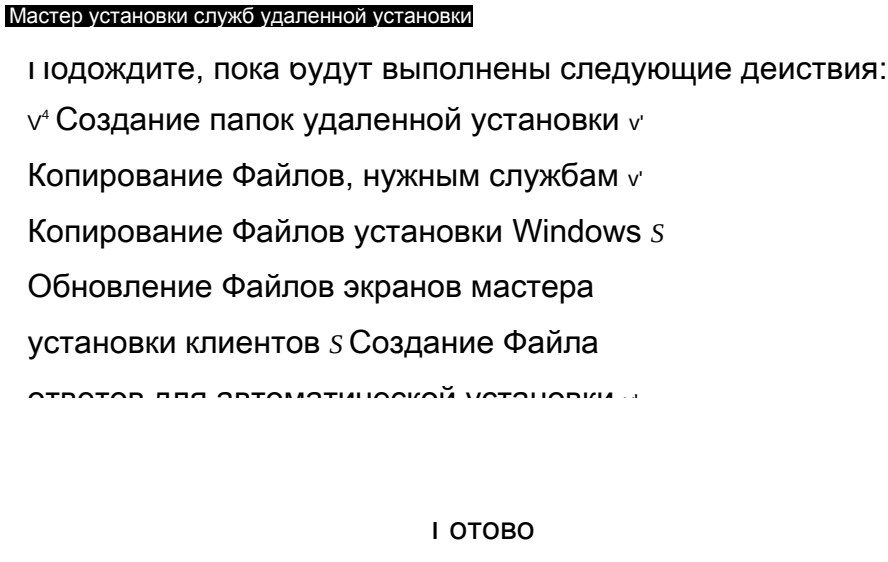


Рис. 2.3. Завершение установки службы RIS

Важно, чтобы сервер RIS прошел авторизацию в Active Directory, об этом сигнализирует последний флажок «DHCP-авторизация» (см. рис. 2.1). Если не авторизовать сервер RIS, то он не сможет отвечать на запросы клиентских компьютеров для сетевой загрузки службы [5].

Необходимо также создать в Active Directory учетную запись пользователя, которой будет разрешено создавать учетные записи компьютеров в домене. Процесс удаленной установки ОС на клиентском компьютере начинается с ввода имени и пароля пользователя, у которого есть такие разрешения.

Важным аспектом выполнения метода удаленной установки является подготовка образов ОС, которые хранятся на отдельном томе сервера RIS. Используя файл ответов для удаленной установки, можно настроить несколько вариантов автоматической установки, которые будут связаны с одним образом ОС, хранящимся на сервере RIS. Для этого необходимо создать соответствующие файлы ответов, в которых можно настроить параметры ОС, конфигурируемые во время ее установки. Файлы ответов для

удаленной установки имеют расширение «.sif», и могут быть созданы с помощью диспетчера установки Windows.

Если на сервере RIS хранится более одного образа, то при запуске мастера установки клиентов загрузится экран выбора образов ОС. Если доступен только один образ ОС, то мастер установки клиентов просто попросит пользователя подтвердить установку. Выбрав один из образов ОС, появляется сообщение о том, что на данный компьютер будет установлена ОС, существующие разделы будут удалены, а жесткий диск будет отформатирован и все данные, находящиеся на диске будут стерты [5].

Как видим из всего выше перечисленного, выполнение метода удаленной установки имеет много нюансов и требует большой подготовки для его реализации. Однако, выполнив установку и настройку сервера RIS один раз, и проведя его апробацию на тестовом клиентском компьютере, ваша сетевая инфраструктура приобретет незаменимый и очень полезный сервис. Процесс удаленной установки клиентских ОС Windows XP Professional с помощью сервера RIS требует минимум участия от пользователя.

2.3. Создание файлов ответов для автоматизации процессов развертывания

Для того чтобы методы развертывания, описанные выше, выполнялись успешно, важно правильно составить файлы ответов. В табл. 2.2. представлен список используемых файлов ответов для различных методов автоматической установки ОС Windows XP Professional.

Таблица 2.2

Файлы ответов

Имя файла	**Применение**	**Место расположения**
Unattend.txt	Для выполнения сценария автоматической установки ОС Windows XP Professional.	%systemdrive%\Deploy
Winnt.sif	Для выполнения сценария автоматической установки ОС Windows XP Professional с компакт-диска. Создается переименованием файла Unattend.txt, в который добавляется секция [Data] с соответствующими разделами.	Флоппи-диск A:\
Sysprep.inf	Для использования утилитой Sysprep (см. п. 2.1.3)	%systemdrive%\Sysprep
Winbom.ini	Если утилита Sysprep используется с параметром -factory, то она работает с данным файлом ответов	%systemdrive%\Sysprep
*.sif	Для удаленной установки с использованием сервера RIS.	Каждый плоский образ ОС, размещенный на сервере RIS, будет содержать папку \Templates, в которой должны

находиться связанные с образом файлы ответов автоматической установки

2.3.1. *Использование диспетчера установки Windows*

Диспетчер установки Windows (Windows Setup Manager) упрощает создание файлов ответов и исключает в них возникновение синтаксических ошибок. Диспетчер установки Windows входит в состав компакт-диска с ОС Windows XP Professional (архив \Support\Tools\Deploy.cab), а также в состав пакета Microsoft Windows XP Resource Kit [2].

Когда вы запускаете диспетчер установки Windows, на экран выводится первая страница мастера диспетчера установки Windows (см. рис. 2.4).

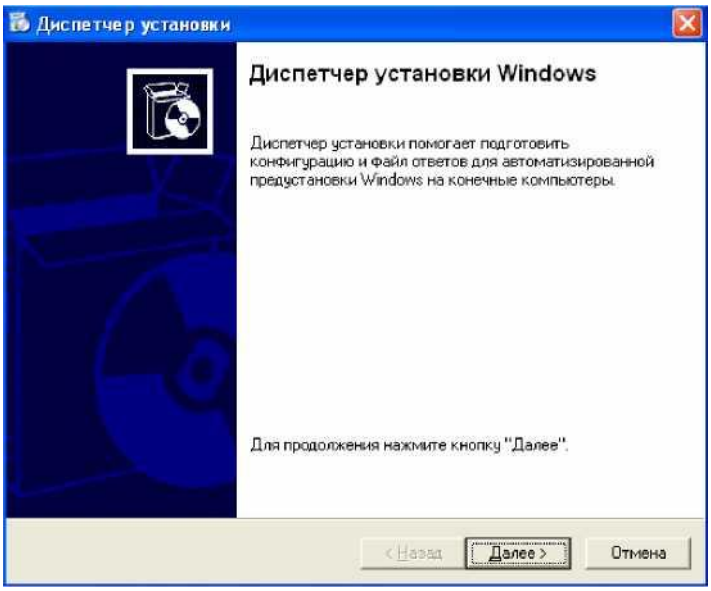


Рис. 2.4. Первая страница мастера диспетчера установки Windows

Щелкните кнопку «Далее», чтобы перейти к следующей странице, на которой следует сделать выбор:

- Создать новый файл ответов;
- Изменить существующий файл ответов.

Если выберите пункт «Создать новый файл ответов», то далее необходимо выбрать тип создаваемого файла ответов. Диспетчер установки Windows может создавать файлы ответов всех типов, представленных в табл. 2.2:

- Для автоматической установки Windows;
- Для установки Sysprep;
- Для служб удаленной установки.

Выбрав нужный вам тип, создайте файл ответов, следуя инструкциям, появляющимся на экране (см. рис. 2.5).

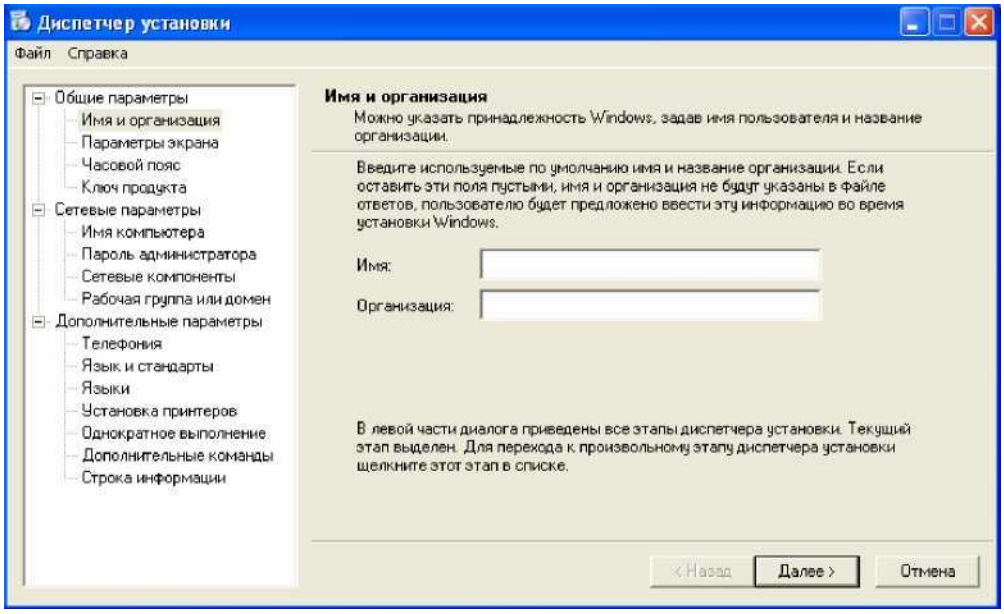


Рис. 2.5. Создание файла ответов в диспетчере установки Windows

2.3.2. *Формат и параметры файла ответов*

Все типы файлов ответов, используемые для автоматической установки Windows XP Professional имеют текстовый формат и похожую структуру, которая состоит из секций содержащих параметры:

```
[Имя секции]
Параметр1 = Значение
Параметр2 = Значение
```

В табл. 2.3 представлен листинг файла ответов Sysprep.inf с пояснениями всех параметров, который был создан с помощью диспетчера установки Windows.

Таблица 2.3

Содержание файла ответов Sysprep.inf

Листинг файла ответов Sysprep.inf	*Пояснения*
;SetupMgrTag **[Unattended]** OemSkipEula=Yes InstallFilesPath=C:\sysprep\i386	**Настройки для запуска процесса установки** Пропуск вывода окна принятия лицензионного соглашения Путь к папке с установочными файлами на компьютере
[GuiUnattended] AdminPassword=* EncryptedAdminPassword=NO OEMSkipRegional=1 TimeZone=201 OemSkipWelcome=1	**Настройки, вводимые через графический пользовательский интерфейс при обычной установке** Пароль администратора остался пустым Пароль не шифруется в файле ответов Пропускаем диалог для установки региональных настроек Часовой пояс - (GTM+06:00 Омск, Новосибирск, ...) Пропуск окна приветствия при входе в систему
[UserData] ProductKey=XXXXX-XXXXX-XXXXX-XXXX FullName="User" OrgName="SibADI" ComputerName=Comp01	**Сведения о пользователе** Ключ лицензионного соглашения Имя пользователя Название организации Имя компьютера
[Display]	**Параметры экрана**

BitsPerPel=32	Число бит на пиксель
Xresolution=1024	Разрешение по горизонтали
YResolution=768	Разрешение по вертикали
Vrefresh=60	Частота вертикальной развертки
[TapiLocation]	**Настройки телефонной связи (Telephony API)**
CountryCode=7	Код страны - 7 (Россия)
AreaCode=3812	Код города - 3812 (Омск)
[RegionalSettings]	**Региональные параметры**
LanguageGroup=5	Используемая языковая группа - Кириллица
SystemLocale=00000419	Системная раскладка клавиатуры - Русская
UserLocale=00000419	Пользовательская раскладка клавиатуры - Русская
InputLocale=0419:00000419	Порядок использования раскладок клавиатуры
[Identification]	**Настройки сетевой идентификации уомпьютера**
JoinDomain=SibADI	Присоединить компьютер к домену «SibADI»
[Networking]	**Настройки сети**
InstallDefaultComponents=Yes	Принимаем сетевые настройки по умолчанию

2.4. Решение Microsoft для развертывания настольных бизнессистем

В последнее время многие компании, имеющие значительный парк компьютеров, сталкиваются с проблемой обновления системного и прикладного ПО. Особенно остро стоит вопрос в целесообразности перехода на новые версии операционных систем и офисных пакетов Microsoft. Ведь помимо финансовых и временных затрат, существуют риски, связанные с несовместимостью используемых приложений с новым базовым ПО, со сбоями в уже налаженном механизме обработки данных и т.д.

Компания Microsoft выпустила комплексное программное решение Business Desktop Deployment (BDD). По своей сути BDD - это набор методических указаний и правил, основанных на концепции Microsoft Solution Framework для планирования, построения, тестирования и развертывания рабочих мест пользователей в рамках корпоративной сетевой инфраструктуры [3].

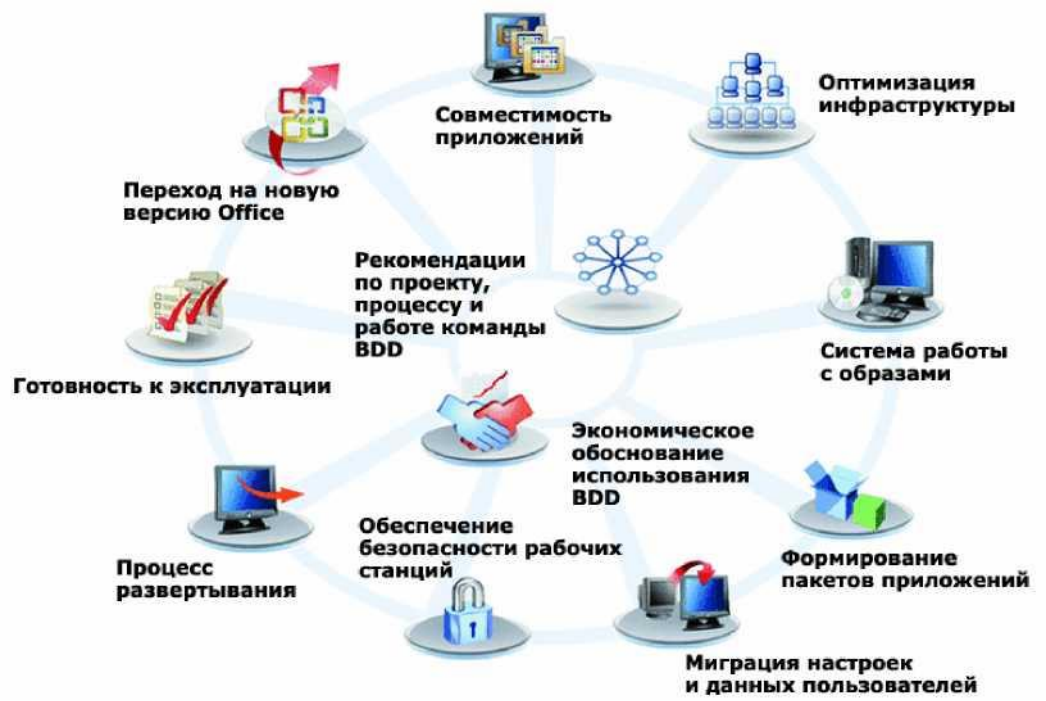


Рис. 2.6. BDD разделяет процесс развертывания настольных бизнес-систем на конкретные задачи.

BDD предлагает целостную систему управления развертыванием и обновлением рабочих мест пользователей. Схематично эта система представлена на рис. 2.6. Она включает в себя комплекс документов, описывающих типовые задачи и процессы управления рабочими местами, руководство по совместимости приложений, руководства по устранению неисправностей инфраструктуры, систему создания и поддержки эталонных образов, средства создания основных и вспомогательных пакетов приложений, средства миграции пользователей, настройки защиты рабочих станций, а также рекомендации по организации внедрения, обеспечения доступности и обновления систем [7].

Если вы серьезно заинтересовались решением проблем развертывания сетевой инфраструктуры на основе ОС Windows 2003/XP в своей организации, то рекомендуем установить и изучить набор руководств и инструментальных средств BDD от компании Microsoft (доступен для бесплатной загрузки с сайта Microsoft).

2.5. Лабораторная работа № 1. Применение утилиты Sysprep для развертывания Windows XP Professional.

На этой лабораторной работе вы подготовите тестовый компьютер для создания образа диска, с которого далее установите ОС Windows XP Professional. Все упражнения данной лабораторной работы № 2А выполняются на виртуальной машине с ОС Windows XP Professional, созданной на предыдущей лабораторной работе.

2.5.1. *Упражнение 1. Извлечение инструментальных средств развертывания Windows XP Professional*

Вы извлечете инструментальные средства развертывания, используемые для автоматической установки Windows XP Professional, и скопируете их на жесткий диск.

1. На виртуальной машине загрузите ОС Windows XP Professional.
2. Зарегистрируйтесь в системе как пользователь с правами администратора.
3. Вставьте установочный компакт-диск Windows XP Professional в привод CD-ROM.
4. Закройте окно «Добро пожаловать в Microsoft Windows XP», выводимое при автозапуске.
5. С помощью Проводника Windows создайте папку C:\Deploy, которая будет использоваться для хранения инструментальных средств развертывания.
6. С помощью Проводника Windows откройте на установочном компактдиске Windows XP Professional папку \Support\Tools\.
7. Дважды щелкните значок файла-архива Deploy.cab. Проводник Windows отобразит содержимое архива Deploy.cab.
8. Отметьте все файлы, содержащиеся в Deploy.cab и извлеките в папку C:\Deploy.

2.5.2. *Упражнение 2. Использование диспетчера установки Windows для создания файла ответов Sysprep.inf*

9. Откройте папку C:\Deploy и щелкните дважды на файл Setupmgr.exe. Запустится диспетчер установки.
10. Появится первая страница мастера диспетчера установки Windows (см. рис. 2.4). Нажмите кнопку «Далее».
11. В появившемся окне «Новый или существующий файл ответов» установите переключатель «Создать новый файл ответов» и нажмите кнопку «Далее».
12. Появится окно, где нужно выбрать тип установки. Установите переключатель «Установка Sysprep» и нажмите кнопку «Далее».
13. Мастер диспетчера установки Windows выводит страницу «Продукт». Убедитесь, что выбран переключатель «Windows XP Professional» и нажмите кнопку «Далее».
14. Появится окно «Лицензионное соглашение». Чтобы использовать полностью автоматическую установку, необходимо принять условия лицензионного соглашения (End-User License Agreement), выбрав соответствующий переключатель и нажав кнопку «Далее».
15. Начинается запись данных в файл ответов sysprep.inf. Сначала необходимо ввести имя пользователя и название вашей организации в соответствующих текстовых полях. Введите в полях «Имя:» и «Организация:»

значения «Student» и «Academy» соответственно и нажмите кнопку «Далее».

16. Оставьте на странице «Параметры экрана» предложенные по умолчанию параметры и нажмите кнопку «Далее».
17. Далее выберите требуемый часовой пояс и нажмите кнопку «Далее». Откроется страница «Ключ продукта».
18. Введите ключ продукта и нажмите кнопку «Далее».
19. Мастер диспетчера установки Windows выводит страницу «Имя компьютера». По умолчанию переключатель установлен на автоматическую генерацию имени компьютера. Выберите переключатель «Использовать следующее имя:», назвав компьютер «Client01», затем нажмите кнопку «Далее».
20. Откроется страница «Пароль администратора», на которой доступен только один переключатель - «Использовать следующий пароль администратора (не более 127 символов)». Не оставляйте пароль администратора пустым! Задайте пароль: **`Password`** и установите флажок «Шифровать пароль администратора в файле ответов». Нажмите кнопку «Далее».
21. Выводится страница «Сетевые компоненты», на которой доступны два переключателя «Обычные параметры» и «Особые параметры». Оставьте значение по умолчанию «Обычные параметры» и нажмите кнопку «Далее».
22. На странице «Рабочая группа или домен» также оставьте значение по умолчанию, указывающее, что компьютер входит в рабочую группу с именем «WORKGROUP».
23. Следующая страница - «Телефония». Введите в поле «Страна:» - «Россия», остальные поля оставьте пустыми. Нажмите кнопку «Далее».
24. Мастер диспетчера установки Windows выводит страницу «Языки и стандарты». По умолчанию выбран переключатель «Выбрать региональные стандарты, используемые по умолчанию для устанавливаемой версии Windows». Нажмите кнопку «Далее», чтобы принять заданные по умолчанию параметры.
25. Выводится страница «Языки», позволяющая вам установить поддержку других языков. В окне «Языки и языковые группы:» выберите щелчком «Кириллица», затем нажмите кнопку «Далее».
26. Затем последовательно выводятся страницы «Установка принтеров», «Однократное выполнение» и «Дополнительные команды». Везде нажмите кнопку «Далее» не вводя никаких значений.
27. На последней странице «Строка информации» можно ввести текст, который запишется в реестр на всех дублируемых компьютерах для упрощения идентификации образов Sysprep. Введите «Лабораторная работа 1» и нажмите кнопку «Готово».

28. Мастер диспетчера установки Windows выводит диалоговое окно, сообщающее, что диспетчер установки успешно создал файл ответов. Нажмите кнопку «ОК», чтобы принять предложенные по умолчанию имя файла и размещение. Закройте диспетчер установки Windows.
29. Откройте созданный вами файл ответов Sysprep.inf в папке C:\Deploy. Обратите внимание, что пароль администратора не хранится в открытом виде (параметр «AdminPassword»). Убедитесь также, что диспетчер установки Windows создал папку Sysprep в корневом разделе образа диска и поместил в нее копию файла Sysprep.inf.

2.5.3. Упражнение 3. Подготовка системы для создания образа диска

Вы выполните подготовку системы для создания образа диска на виртуальной машине с ОС Windows XP Professional. Перед выполнением этого упражнения можно установить какое-нибудь прикладное программное обеспечение на данной виртуальной машине.

1. Вы зарегистрированы в системе как пользователь с правами администратора.
2. Откройте папку C:\Deploy и щелкните дважды на файл Sysprep.exe.
3. Выводится диалоговое окно «Программа подготовки системы 2.0», предупреждающее, что запуск программы Sysprep может привести к изменению некоторых параметров безопасности. Для продолжения работы нажмите кнопку «ОК».
4. Далее выводится окно, позволяющее вам настроить параметры Sysprep. В группе параметров «Флаги» пометьте флажок «Мини-установка», а затем нажмите кнопку «Запечатать компьютер».
5. Sysprep выводит окно, сообщающее что вы выбрали регенерацию дескрипторов безопасности (SID) при следующей перезагрузке компьютера. Нажмите кнопку «ОК».
6. Откроется окно «Работает Sysprep...». Через некоторое время ваш компьютер завершит работу.
7. Вы создали образ диска, который теперь можно копировать на другие компьютеры с помощью специального ПО для клонирования дисков. В рамках лабораторной работы для экономии времени пропустим этот шаг.

2.5.4. Упражнение 4. Установка Windows XP Professional с образа диска

В этом упражнении вы будете использовать созданный ранее образ диска для развертывания ОС Windows XP Professional с предустановленным прикладным ПО. Установку образа будем выполнять на тот же компьютер, на котором создавали образ.

1. Включите компьютер, на котором был создан образ. Программа установки через некоторое время выводит следующее сообщение «Please Wait While Windows Prepares To Start».

2. Если утилита Sysprep обнаружит созданный вами файл ответов Sysprep.inf в папке C:\Sysprep, то на экране появится окно «Установка Windows XP» (см. рис. 2.2), в котором будет сообщение «Пожалуйста, подождите». В противном случае появится первая страница мастера установки Windows XP Professional, и вам придется выполнить процедуру мини-установки вручную.
3. Программа установки считает данные из файла ответов Sysprep.inf. При этом на экране в окне «Установка Windows XP» галочками будут отмечаться выполненные действия.
4. После окончания установки XP Professional зарегистрируйтесь как Администратор.
5. Выберите «Пуск», на ярлыке «Мой компьютер» нажмите правую кнопку мыши, в контекстном меню перейдите на «Свойства». В появившемся окне «Свойства системы» на вкладке «Общие» вы увидите, что имя пользователя и название организации установлено из файла ответов: «Student» и «Academy».
6. Перейдите на следующую вкладку «Имя компьютера» окна «Свойства системы». Убедитесь, что имя компьютера «Client01» и он входит в рабочую группу «WORKGROUP». Закройте окно «Свойства системы».
7. Выберите «Пуск» / «Выполнить». Запусти программу «Редактор реестра», набрав в поле запуска «regedit».
8. В левой навигационной панели программы «Редактор реестра» перейдите в раздел «HKEY_LOCAL_MACHINE\SYSTEM\Setup». Убедитесь, что значением параметра «OEMDuplicatorString» является запись из файла ответов «Лабораторная работа 1».

2.5.5. Самостоятельное упражнение. Автоматическая установка Windows XP Professional с компакт-диска

С помощью диспетчера установки Windows создайте файл ответов для автоматической установки Windows XP Professional с компакт-диска. Сравните содержимое вашего файла ответов Winnt.sif с созданным в упражнении № 2 - Sysprep.inf. Скопируйте файл ответов Winnt.sif на дискету и выполните самостоятельно установку ОС Windows XP Professional с компакт-диска.

2.6. Лабораторная работа № 2. Проведение удаленной установки ОС Windows XP Professional

На этой лабораторной работе вы установите службу RIS на компьютер с серверной ОС Windows Server 2003, с помощью которой далее удаленно установите ОС Windows XP Professional на новый компьютер. Упражнения данной лабораторной работы выполняются на виртуальных машинах с ОС Windows Server 2003 и с ОС Windows XP Professional, созданных ранее.

2.6.1. *Упражнение 1. Подготовка виртуальной машины с ОС Windows Server 2003 для установки службы RIS*

Ознакомьтесь с требованиями для проведения метода удаленной установки (раздел 2.2.1). На созданной в ходе лабораторной работы №1 виртуальной машине с серверной ОС Windows Server 2003, установлены требуемые сетевые службы: DNS, DHCP и Active Directory. Обязательным условием также является наличие дополнительного общего тома, отформатированного под файловую систему NTFS версии 5 и выше. В этом упражнении создадим этот дополнительный том, на котором потом будут храниться образы устанавливаемых ОС.

1. Добавьте дополнительный жесткий диск размером 2 Гб к виртуальной машине с Windows Server 2003.
2. На виртуальной машине загрузите ОС Windows Server 2003.
3. Зарегистрируйтесь в системе под учетной записью администратора домена Test.
4. Выберите «Пуск», на ярлыке «Мой компьютер» нажмите правую кнопку мыши, в контекстном меню перейдите на «Управление». В появившемся окне «Управление компьютером» выберите оснастку «Управление дисками».
5. Запустится мастер инициализации и преобразования дисков. Нажмите кнопку «Далее».
6. Появится окно «Выбор диска для инициализации», в котором будет отмечен «Диск 1». Нажмите кнопку «Далее».
7. В следующем окне «Выбор дисков для преобразования» отметьте «Диск 1» и нажмите кнопку «Далее».
8. В появившемся окне «Завершение мастера инициализации» нажмите кнопку «Готово». В оснастке «Управление дисками» убедитесь, что состояние присоединенного диска «Подключен».
9. Теперь на подключенном диске необходимо создать новый раздел. Правой клавишей мыши щелкните в нераспределенную область (черного цвета) диска «Диск 1», в появившемся меню выберите «Создать раздел». (Если появится пункт «Создать том», то это означает, что присоединенный диск использует динамическое хранение. Правой клавишей мыши щелкните на иконку «Диск 1» и выберите в меню пункт «Преобразовать в базовый диск». Теперь выполните пункт 9 этого упражнения).
10. Запустится мастер создания разделов. Нажмите кнопку «Далее».
11. В окне «Выбор типа раздела» оставьте вариант «Основной раздел» и нажмите кнопку «Далее».
12. В появившемся окне «Указание размера раздела» ничего не меняйте, оставьте предложенный размер и нажмите кнопку «Далее».

13. В следующем окне «Назначение буквы диска или пути» установите переключатель на вариант «Назначить букву диска (A-Z):» и выберите букву «R». Нажмите кнопку «Далее».
14. Откроется окно «Форматирование раздела». По умолчанию переключатель стоит на варианте «Форматировать данный раздел следующим образом:». Выбрана файловая система «NTFS», размер кластера - «По умолчанию». Задайте метку тома «RIS» и установите флажок «Быстрое форматирование». Нажмите кнопку «Далее».
15. В появившемся окне «Завершение мастера создания раздела» нажмите кнопку «Готово». Вы увидите, что область диска стала синего цвета, и «Диск 1» быстро форматируется под файловую систему NTFS.
16. Закройте окно «Управление компьютером». С помощью проводника Windows убедитесь, что у вас появился диск R с меткой «RIS».

2.6.2. Упражнение 2. Установка службы удаленной RIS

1. Вставьте установочный компакт-диск Windows Server 2003 в CD-ROM.
2. В Windows Server 2003, нажмите «Пуск», выберите «Настройка» и перейдите в «Панель Управления».
3. Откройте элемент «Установка и удаление программ». Слева на панели нажмите на кнопку «Установка компонентов Windows».
4. Прокрутите список, выберите «Службы удаленной установки» и нажмите кнопку «Далее». Начнется установка службы RIS на ваш сервер.
5. Нажмите кнопку «Готово» для выхода из мастера компонентов Windows.
6. Вам будет предложено перезагрузить компьютер. Нажмите кнопку «Да».
7. После перезагрузки сервера войдите в систему под учетной записью администратора домена.
8. Выберите «Пуск» / «Программы» / «Администрирование» / «Установка служб удаленной установки». Запустится мастер установки служб удаленной установки. Появится экран приветствия, в котором перечислены некоторые требования для успешной установки службы RIS. Нажмите кнопку «Далее».
9. В следующем окне вам будет предложено указать диск и папку на сервере, где будут размещены файлы RIS. По умолчанию эта папка размещается на самом большом, несистемном, незагрузочном, разделе, отформатированном в файловой системе NTFS. В нашем случае это будет R:\RemoteInstall. Нажмите кнопку «Далее».
10. Далее появится окно «Исходные параметры», где можно сразу включить обслуживание сервером RIS клиентских компьютеров. Выберите только параметр «Отвечать на запросы клиентских компьютеров» и нажмите кнопку «Далее».

11. Далее нужно указать местонахождение установочных файлов ОС Windows XP Professional. Вставьте установочный компакт-диск Windows XP Professional в CD-ROM и введите букву CD-привода. Нажмите кнопку «Далее».
12. Далее вам будет предложено ввести имя папки, в которой будут содержаться установочные файлы ОС Windows XP Professional на сервере. Эта папка будет создана внутри папки R:\RemoteInstall. По умолчанию предлагается имя «WINDOWS». Оставьте имя папки без изменений и нажмите кнопку «Далее».
13. Далее необходимо ввести понятное описание и текст подсказки для образа установки Windows XP Professional на английском языке (символы кириллицы не поддерживаются мастером установки клиентов). Описание и поясняющий текст будут отображаться в процессе установки на удаленный компьютер. В данном упражнении ничего менять не будем, но на практике подсказка должна быть понятной для пользователей, чтобы они смогли выбрать правильный вариант во время установки. Нажмите кнопку «Далее», чтобы сохранить название по умолчанию «Microsoft Windows XP Professional RU».
14. В последнем окне отобразятся выбранные вами параметры для сервера удаленной установки. Нажмите кнопку «Готово», чтобы завершить установку сервера RIS.
15. Дождитесь, пока мастер установит выбранные службы и настройки. Это займет несколько минут. После завершения процесса появится экран, представленный на рис. 2.3. Нажмите кнопку «Готово».

2.6.3. Упражнение 3. Создание загрузочной дискеты

Загрузочная дискета необходима для запуска удаленной установки ОС Windows XP Professional на клиентском компьютере, так как в BIOS Virtual PC нельзя выбрать сетевой адаптер в качестве устройства с которого можно начать загрузку.

1. Вставьте в дисковод чистую отформатированную дискету.
2. С помощью проводника Windows перейдите в папку R:\RemoteInstall\Admin\i386.
3. Запустите файл rbfg.exe для старта утилиты «Генератор дисков удаленной установки». Прочитайте выведенную в окне информацию и нажмите кнопку «Создать диск».
4. Далее появится диалоговое окно, предлагающее создать еще одну загрузочную дискету. Нажмите кнопку «Нет».
5. Нажмите кнопку «Закрыть», чтобы закрыть окно «Дискета удаленной загрузки для Microsoft Windows».

2.6.4. Упражнение 4. Создание файла ответов для автоматической удаленной установки

Будем создавать файл ответов для автоматической удаленной установки на виртуальной машине с ОС Windows XP Professional, использовавшейся в лабораторной работе №2.

1. Откройте папку C:\Deploy, куда были извлечены файлы из архива Deploy.cab, и щелкните дважды на файл Setupmgr.exe. Запустится диспетчер установки.
2. Появится первая страница мастера диспетчера установки Windows. Нажмите кнопку «Далее».
3. В появившемся окне «Новый или существующий файл ответов» установите переключатель «Создать новый файл ответов» и нажмите кнопку «Далее».
4. Появится окно, где нужно выбрать тип установки. Установите переключатель «Службы удаленной установки (RIS)» и нажмите кнопку «Далее».
5. Мастер диспетчера установки Windows выводит страницу «Продукт». Убедитесь, что выбран переключатель «Windows XP Professional» и нажмите кнопку «Далее».
6. В окне «Взаимодействие с пользователем» выберите вариант «Полностью автоматическая установка» и нажмите кнопку «Далее».
7. Появится окно «Лицензионное соглашение». Чтобы использовать полностью автоматическую установку, необходимо принять условия лицензионного соглашения (End-User License Agreement), отметив флажок «Я принимаю условия лицензионного соглашения». Нажмите кнопку «Далее».
8. Начинается запись данных в файл ответов. Сначала необходимо ввести имя пользователя и название вашей организации в соответствующих текстовых полях. Введите в полях «Имя:» и «Организация:» значения «Student» и «Academy» соответственно и нажмите кнопку «Далее».
9. Оставьте на странице «Параметры экрана» предложенные по умолчанию параметры и нажмите кнопку «Далее».
10. Далее выберите требуемый часовой пояс и нажмите кнопку «Далее». Откроется страница «Ключ продукта».
11. Введите ключ продукта и нажмите кнопку «Далее».
12. Откроется страница «Пароль администратора», на которой доступен только один переключатель - «Использовать следующий пароль администратора (не более 127 символов)». Не оставляйте пароль администратора пустым! Задайте пароль: **`Password`** и установите флажок «Шифровать пароль администратора в файле ответов». Нажмите кнопку «Далее».
13. Выводится страница «Сетевые компоненты», на которой доступны два переключателя «Обычные параметры» и «Особые параметры». Оставь

те значение по умолчанию «Обычные параметры» и нажмите кнопку «Далее».

14. Следующая страница - «Телефония». Введите в поле «Страна:» - «Россия», остальные поля оставьте пустыми. Нажмите кнопку «Далее».
15. Мастер диспетчера установки Windows выводит страницу «Языки и стандарты». По умолчанию выбран переключатель «Выбрать региональные стандарты, используемые по умолчанию для устанавливаемой версии Windows». Нажмите кнопку «Далее», чтобы принять заданные по умолчанию параметры.
16. Выводится страница «Языки», позволяющая вам установить поддержку других языков. В окне «Языки и языковые группы:» выберите щелчком «Кириллица», затем нажмите кнопку «Далее».
17. В окне «Параметры обозревателя и оболочки» оставьте вариант «Использовать для настройки обозревателя параметры по умолчанию» и нажмите кнопку «Далее».
18. Папку установки оставьте предлагаемую по умолчанию «... с именем Windows», нажмите кнопку «Далее».
19. Затем последовательно выводятся страницы «Установка принтеров», «Однократное выполнение» и «Дополнительные команды». Везде нажмите кнопку «Далее» не вводя никаких значений.
20. На последней странице «Текст информационного файла установки» необходимо ввести понятное описание и текст справки для образа установки Windows XP Professional на английском языке (символы кириллицы не поддерживаются мастером установки клиентов). Введите в поле описания - «Windows XP Professional - Lab2», а в поле справки - «Remote installation Windows XP Professional», затем нажмите кнопку «Готово».
21. Мастер диспетчера установки Windows выводит диалоговое окно, сообщающее, что диспетчер установки успешно создал файл ответов. Нажмите кнопку «ОК», чтобы принять предложенные по умолчанию имя файла и размещение C:\windist\remboot.sif. Закройте диспетчер установки Windows.
22. Скопируйте файл remboot.sif с виртуальной машины ОС Windows XP Professional из папки C:\windist\ на виртуальную машину ОС Windows Server 2003 в корень на диск C:\.

2.6.5. Упражнение 5. Настройка сервера удаленной установки

В этом упражнении вы проверите авторизацию сервера RIS в Active Directory, создадите пользователя, у которого будет разрешение добавлять учетные записи компьютеров в домен Test. Вы также свяжите созданный в предыдущем упражнении файл ответов remboot.sif с уже имеющимся образом ОС Windows XP Professional для удаленной установки. Упражнение выполняется на виртуальной машине с ОС Windows Server 2003.

1. Зарегистрируйтесь на сервере как пользователь с правами администратора домена.
2. Выберите «Пуск» / «Программы» / «Администрирование» / оснастка «DHCP». Запустите оснастку.
3. Правой кнопкой мыши щелкните по значку «DHCP» в верхнем левом углу оснастки и выберите в контекстном меню пункт «Список авторизованных серверов...». Убедитесь, что ваш сервер авторизован. Если список в окне «Авторизованные DHCP-серверы:» пуст, нажмите кнопку справа «Авторизовать» и введите IP адрес сервера RIS. Нажмите кнопку «Да», когда потребуется подтвердить правильность адреса.
4. Выберите «Пуск» / «Программы» / «Администрирование» / оснастка «Active Directory - пользователи и компьютеры». Запустите оснастку.
5. Перейдите в контейнер «Users». В правом окне оснастки появится список пользователей и групп домена Test.local. В меню «Действие» выберите пункт «Создать» / «User».
6. Откроется окно «Новый объект - User». В полях «Имя:» и «Имя входа пользователя:» введите «Lab2User», затем нажмите кнопку «Далее».
7. В следующем окне задайте пароль для пользователя Lab2User - **`PasswOrd`** и снимите флажок «Требовать смену пароля при следующем входе в систему». Нажмите кнопку «Далее».
8. Появится итоговое окно, в котором вы увидите полное имя и имя входа пользователя. Убедитесь, что в именах нет ошибок, и нажмите кнопку «Готово».
9. Далее пользователю Lab2User нужно дать необходимые разрешения на создание учетных записей компьютеров в домене Test.local. Правой кнопкой мыши щелкните на значок имени домена Test.local в левом окне оснастки, и выберите пункт «Делегирование управления».
10. Запустится мастер делегирования управления. Нажмите кнопку «Далее».
11. В появившемся окне «Пользователи или группы» нажмите кнопку «Добавить» для добавления пользователя, которому будет разрешено производить удаленную установку ОС на компьютеры при помощи службы RIS.
12. В появившемся окне введите имя пользователя - Lab2User и нажмите кнопку «ОК».
13. Убедитесь, что в следующем окне поле «Выбранные пользователи и группы:» содержит объект пользователя с именем «Lab2User (Lab2User@Test.local)», и нажмите кнопку «Далее».
14. В окне «Делегируемые задачи» отметьте пункт «Присоединение компьютера к домену» и нажмите кнопку «Далее».
15. В последнем окне мастера нажмите кнопку «Готово».
16. Далее необходимо связать файл ответов remboot.sif, который лежит в корне на диске C:\ с образом ОС Windows XP Professional для удален

ной установки. В левом окне открытой ранее оснастки «Active Directory - пользователи и компьютеры» перейдите в контейнер «Domain Controllers».

17. В правом окне оснастки откроется список контроллеров домена Test.local, состоящий из одного сервера с именем Server01. Нажмите правой клавишей мыши на значок Server01 в появившемся контекстном меню выберите пункт «Свойства».
18. Перейдите на вкладку «Удаленная установка». На этой вкладке нажмите кнопку «Дополнительные параметры». Откроется окно «Свойства: Server01-Remote-Installation-Services», вкладка «Новые клиенты».
19. Перейдите на вкладку «Образы». Вы увидите, что у вас имеется один образ ОС, созданный ранее с описанием «Microsoft Windows XP Professional RU» (см. п.13 упражнения 2). Нажмите кнопку «Добавить».
20. В открывшемся окне оставьте вариант «Сопоставить новый файл ответов существующему образу» и нажмите кнопку «Далее».
21. В окне «Источник файла ответов для автоматической установки» выберите вариант «Иное место» и нажмите кнопку «Далее».
22. В следующем окне «Выбор образа установки» щелкните левой кнопкой мыши на единственный имеющийся у вас образ и нажмите кнопку «Далее».
23. В появившемся окне укажите путь к созданному в упражнении 4 файлу ответов - C:\remboot.sif (можно воспользоваться кнопкой «Обзор»). Нажмите кнопку «Далее».
24. Задайте понятное описание и текст справки для образа установки Windows XP Professional. Помните, что символы кириллицы не поддерживаются мастером установки клиентов. Введите в поле описания - «Win- dows XP Professional - Lab2», а в качестве поясняющего текста - «Re- mote installation Windows XP Professional», затем нажмите кнопку «Далее».
25. Последнее окно «Просмотр параметров» позволяет просмотреть, куда был скопирован ваш файл ответов в поле «Конечный путь». Нажмите кнопку «Готово».
26. Убедитесь, что добавлен новый образ с описанием «Windows XP Profes- sional - Lab2» и нажмите кнопку «ОК» на вкладке «Образы».
27. В окне «Свойства: Server01» можете нажать кнопку «Проверить сервер», чтобы еще раз удостовериться, что сервер RIS авторизован и запускаются требуемые службы удаленной установки. Убедитесь также, что в области «Поддержка клиентов» включен только флажок «Отвечать клиентским компьютерам, запрашивающим обслуживание». Нажмите кнопку «ОК» и закройте оснастку «Active Directory - пользователи и компьютеры».

2.6.6. Упражнение 6. Выполнение удаленной установки ОС Windows XP Professional на клиентский компьютер

Это упражнение является последним в данной лабораторной работе. Вам предстоит выполнить удаленную установку ОС Windows XP Professional на клиентский компьютер. Вы можете создать новую виртуальную машину и выполнить на нее удаленную установку. Можно взять уже существующую виртуальную машину с ОС Windows XP Professional, и загрузившись с загрузочной дискеты для запуска удаленной установки, выполнить данное упражнение.

1. Вставьте в флоппи-дисковод загрузочную дискету для запуска удаленной установки, созданную в ходе упражнения 3 данной лабораторной работы.
2. Запустите виртуальную машину. Установите в BIOS в качестве первого загрузочного устройства флоппи-диск. Сохраните настройки и выйдите из BIOS.
3. Должна начаться загрузка с дискеты, В случае успешного соединения с DHCP-сервером, компьютер получит IP-адрес и вам будет предложено нажать клавишу «F12» для запуска мастера установки клиентов.
4. Загрузится экран «Client Installation Wizard» в текстовом режиме на синем фоне. Выньте загрузочную дискету из дисковода и нажмите клавишу «Enter» на клавиатуре.
5. Появится следующий экран, где вам нужно ввести учетную запись и пароль пользователя, которому разрешено производить удаленную установку ОС на компьютеры при помощи службы RIS. Введите в соответствующих полях - **`Lab2User`** / **`Password`** и нажмите клавишу «Enter» на клавиатуре.
6. Далее необходимо выбрать нужный образ операционной системы. Наведите курсор на вариант «Windows XP Professional - Lab2» и нажмите клавишу «Enter» на клавиатуре.
7. Появится предупреждение о том, что все данные на жестком диске будут удалены. Нажмите клавишу «Enter».
8. На следующем экране вы увидите имя учетной записи клиентского компьютера, которое генерируется автоматически (по умолчанию на основе имени пользователя), а также уникальный код компьютера GUID. Нажмите клавишу «Enter» на клавиатуре и начнется удаленная установка ОС Microsoft Windows XP Professional.
9. Во время удаленной установки никакого участия от вас не потребуется. Все настройки ОС будут выполнены в соответствии с файлом ответов.

2.7. Закрепление материала

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

1. Для политики безопасности организации выполнение быстрого развертывания сетевой инфраструктуры обеспечивает:
   a) целостность;
   b) доступность;
   c) конфиденциальность.

2. Какая утилита Microsoft играет главную роль в методе дублирования дисков:
   a) setupmgr.exe;
   b) sysprep.exe;
   c) rbfg.exe.

3. Как должен называться файл ответов для удаленной установки ОС с помощью сервера RIS?
   a) unattend.txt;
   b) winboom.ini;
   c) sysprep.inf;
   d) Любое имя файла с расширением *.sif

4. Какие сетевые службы необходимы для работы сервера RIS?

5. Отметьте правильные утверждения, касающиеся метода удаленной установки:
   a) Клиентский компьютер должен быть совместим с PXE boot ROM;
   b) На клиентском компьютере должна быть предустановленна любая ОС Microsoft;
   c) Для хранения файлов RIS необходим общий том с файловой системой NTFS версии 5 или выше;
   d) RIS-сервер может быть создан только на сервере, являющимся контроллером домена.

Тема: Обеспечение безопасности хранения данныхв ОС Microsoft

На этом занятии рассмотрим один из ключевых моментов информационной безопасности любой организации – это обеспечение сохранности данных. Под данными будем понимать различные пользовательские файлы, которые постоянно создаются, редактируются и удаляются в процессе функционирования организации. В этих файлах может храниться информация любой важности: от несущественной, утрата которой никак не скажется на бизнес-процессах, до критичной, потеряв которую компания рискует закончить свое существование.

В рамках этого занятия не будем касаться вопроса классификации данных по степени их важности. По этой тематике есть много литературы из области теории информационной безопасности, управления рисками и т.п.

Цель этого занятия ознакомиться с предоставляемыми возможностями ОС Microsoft Windows 2003/XP по обеспечению безопасности хранения данных в целом, не смотря на их степень значимости.

Из теории информационной безопасности известно, что обеспечение сохранности информации достигается различными решениями: начиная с тиражирования информационных ресурсов (программ и данных) и заканчивая резервированием устройств хранения данных [4]. Поэтому на данном занятии рассмотрим интересные и полезные решения, предоставляемые ОС Microsoft Windows 2003/XP в этом диапазоне:

- технология теневого копирования данных;
- архивация данных;
- создание отказоустойчивых томов для хранения данных.

Прежде всего

Для изучения материалов этой главы необходимы следующие ресурсы:

- Компьютер под управлением операционной системы Windows XP Professional с параметрами по умолчанию, объемом оперативной памяти не менее 1 Гб и сетевой картой.
- Свободное место на жестком диске не менее 8 Гб.

4.1. Технология теневого копирования данных

Суть данной технологии заключается в создании копий выбранных файлов через определенные промежутки времени. Реализована технология в виде отдельной службы теневого копирования тома (VSS). Она используется для управления данными на дисках и может взаимодействовать с

различными приложениями. Например, в программах резервного копирования, эта служба обеспечивает копирование файлов, занятых во время архивации другими приложениями.

Важной практической функцией технологии теневого копирования является возможность восстановления последних версий случайно удален-Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 3

ных или поврежденных файлов. В ОС Microsoft Windows 2003/XP предоставляется возможность пользователям клиентских компьютеров восстанавливать файлы из теневой копии самостоятельно без вмешательства системных администраторов, что, безусловно, очень удобно с точки зрения экономии времени [7].

4.1.1. Ограничения теневого копирования томов

Теневые копии файлов на заданных томах доступны только на серверах под управлением ОС Windows Server 2003. На сервере в каталоге %System-root%\System32\Clients\Twclient\x86\ имеется клиентское ПО для инсталляции на компьютеры под управлением Windows XP Professional, установив которое пользователи смогут получать доступ к теневым копиям через вкладку «Предыдущие версии» окна свойств файлов теневого тома [5]. Последняя версия этого клиентского ПО доступна по адресу: http://www.microsoft.com/windowsserver2003/downloads/shadowcopyclient.mspx.

Теневое копирование тома не будет работать для точек подключения, когда второй жесткий диск подключается к первому в виде папки [2] .

Создавать теневые копии можно только на томах с файловой системой NTFS. Теневое копирование будет выполняться для всех общих папок, хранящихся на этом томе. Возможности выбрать отдельные общие папки на томе, для которых бы создавались теневые копии – нет! Для хранения теневых копий требуется не менее 100 Мб свободного места на выбранном томе [9]. Максимально допустимый значение – 64 теневые копии на один том, независимо от того, сколько свободного места остается в области хранения.

4.1.2. Установка и использование технологии теневого копирования томов

На сервере под управлением ОС Windows Server 2003 желательно разместить общие папки, для которых хотите использовать теневые копии, на

отдельном томе. Это убережет от заполнения теневыми копиями дискового пространства и снижения пропускной способности средств ввода-вывода в результате копирования тех общих папок, для которых функция теневого копирования не нужна [2].

Для активизации создания теневых копий на томе, в окне его свойств перейдите на вкладку «Теневые копии» (см. рис. 4.1).

На этой вкладке следует выбрать том, для общих папок которого будут создаваться теневые копии. При большой загрузке файлового сервера целесообразно хранить теневые копии на отдельном томе, который бы размещался на другом жестком диске. Это повысит производительность сервера.

Рис. 4.1. Вкладка «Теневые копии» окна свойств диска.

По умолчанию теневые копии сохраняются на том же диске, где хранятся общие папки. При этом устанавливаются следующие настройки [2]:

- Максимальный размер места для хранения теневых копий равен 10% от общего пространства диска;
- Автоматически проводить копирование с понедельника по пятницу в 7 утра и в 12 ночи;
- Создается первая теневая копия.

Для изменения настроек теневых копий тома отличных от заданных по умолчанию, выберите нужный том из списка и нажмите кнопку «Параметры» (см. рис 4.2).

Рис. 4.3. Окно настройки параметров теневого копирования тома.

Если вы решили изменить расписание создания теневых копий, нажми-

те кнопку «Расписание» появится окно, представленное на рис. 4.3, для его настройки. Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 6

Рис. 4.3. Окно настройки расписания теневого копирования тома.

После выполненных настроек нажмите кнопку «Включить», и начнут создаваться теневые копии общих папок на заданном томе. Теперь, если обратиться через контекстное меню к свойствам файлов, хранящимся в общих папках, появится специальная вкладка «Предыдущие версии» (см. рис 4.4). Эта вкладка будет доступна в окне свойств файла, только если вы обратились к общей папке как к сетевому ресурсу (например, UNC-путь)! Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 7

Рис. 4.4. Вкладка «Предыдущие версии» в окне свойств общей папки.

Внизу вкладки имеются три кнопки, позволяющие совершать различные действия с копиями файла:

- «Показать» – позволяет просмотреть выбранную копию файла;
- «Копировать» – позволяет копировать выбранную копию файла в новое расположение;
- «Восстановить» – Позволяет восстанавливать выбранную копию файла поверх текущей версии файла.

Далее рассмотрим случай, когда файл был удален и требуется его восстановление из теневой копии. Так как объект файл, на котором можно щелкнуть правой кнопкой мыши, в общей папке в этом случае отсутствует, необходимо обратиться к свойствам папки, где имеется такая же вкладка «Предыдущие версии». Нажав кнопку «Показать», можно просмотреть какие файлы и папки содержались в ней на выбранный момент времени. Отсюда можно восстановить удаленный файл в любое место, в том числе и в

прежнюю папку.

Как видим, процедура восстановления файла из теневой копии достаточно простая и быстрая операция для пользователей. Но следует помнить, что технология теневого копирования не является стопроцентным решени-

ем задачи обеспечения сохранности данных. Она решает проблему быстрого восстановления совместно используемых файлов из общих папок.

4.2. Архивация данных

Под архивацией принято понимать обычное копирование данных на резервный носитель информации, чтобы в случае отказа или повреждения основного устройства хранения, можно было быстро восстановить хранившиеся на нем данные. Архивация обеспечивает наивысшую степень отказоустойчивости по сравнению со всеми другими технологиями хранения данных, обеспечивающих отказоустойчивость, такими как: теневое копирование, избыточные массивы независимых дисков, кластерные серверы и т.д. [5]

Эффективность применения архивации в сетевой инфраструктуре зависит от правильного выбора специального ПО и планирования. В состав ОС Microsoft Windows 2003/XP входит служебная программа Backup, обеспечивающая основные функции архивации, включая возможности работы по расписанию и взаимодействие со службой теневого копирования тома [9].

4.2.1. Работа с программой архивирования Backup

Выполнять архивацию всех данных на компьютере почти никогда не требуется, так как при выходе из строя жесткого диска можно достаточно быстро выполнить установку ОС и основного прикладного ПО (см. занятие 2). Поэтому следует архивировать только создаваемые пользователями файлы (документы, базы данных и т.п.) и файлы конфигурации приложений. Разумный выбор объектов для резервного копирования сэкономит общее время и ресурсы архивации.

Рис. 4.5. Первая страница мастера программы архивирования Buckup

При первом запуске программа архивирования Buckup («Пуск» / «Программы» / «Стандартные» / «Служебные» / «Архивация данных») запускается в режиме мастера (см. рис. 4.5). На этом занятии работа программы Buckup Windows в режиме мастера изучаться не будет. Нажав ссылку «Расширенный режим», а затем, перейдя на вкладку «Архивация» (см. рис. 4.6), отобразится древовидное меню для выбора архивируемых данных. Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 10

http://www.isu.kasib.ru

Рис. 4.6. Вкладка «Архивация» в окне программы Backup Windows

На этой вкладке необходимо выбирать файлы и папки, которые должны быть заархивированы. Выбирая определенную папку (диск), Buckup автоматически помечает к архивации все файлы или папки внутри нее. При этом флажок отметки будет синего цвета. Если нужно исключить какие-то файлы или папки из уже отмеченных, щелкните на связанный с ними флажок и снимите пометки о включении. При этом у родительской папки флажок отметки изменит цвет с синего на серый, что означает не стопроцентный выбор содержимого внутри папки. Используя папку «Сетевое окружение», можно включить в процесс архивации данные с других компьютеров сети.

Слева в нижней части окна нужно задать имя файла-архива и выбрать место его сохранения. Файлы-архивы, создаваемые программой Backup, могут быть размещены на любых носителях информации, таких как жесткие диски, записываемые компакт-диски в форматах CD и DVD, накопители на сменных картриджах (Zip, Jaz) и на магнитной ленте. При этом размер файла-архива будет ограничиваться емкостью используемого носителя. Поэтому целесообразно в сетевой инфраструктуре выделить специальный сервер с большим объемом дискового пространства для хранения архивов. Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 11

После того, как заданы носитель и имя архива, выбраны все необходимые файлы и папки для резервного копирования, щелкните кнопку «Архивировать» для задания параметров архивации и запуска самого процесса. Появится окно «Сведения о задании архивации» (см. рис. 4.7).

Рис. 4.7. Окно «Сведения о задании архивации» программы Backup Windows

В этом окне можно задать описание архива и метку носителя. Если будет выбран вариант «Дозаписать этот архив к данным носителя» (по умолчанию), то значение из текстового поля, где задается метка носителя, не используется, и она останется прежней. Это окно содержит кнопки «Архивировать», «Дополнительно», «Расписание» и «Отмена». Если нажать кнопку «Архивировать», то запустится процесс архивации. Но до этого можно настроить дополнительные параметры и расписание архивации, нажав соответствующие кнопки.

4.2.2. Стратегии архивации

Программа Backup Windows поддерживает пять стандартных типов архивации, которые в действительности представляют собой комбинации фильтров [5]. Для осуществления первых трех типов архивации (см. табл. 4.1) используются атрибуты файлов. Факт изменения файла определяется по установке атрибута «архивный» (бит архива). Во время архивации этот атрибут сбрасывается [8].

Таблица 4.1

Типы архивации

Тип архива	Архивируемые данные	Состояние бита архива
Нормальный	Все выбранные файлы, независимо от того, архивировались ли они ранее.	Сбрасывается

Добавочный
Только файлы, модифицированные с момента последней нормальной или добавочной архивации.
Сбрасывается

Разностный
Только файлы, модифицированные с момента последней нормальной архивации.
Не сбрасывается
Копирующий Все выбранные файлы Не используется
Ежедневный
Только файлы, созданные или модифицированные за текущие сутки
Не используется

Представленные типы архивации в табл. 4.1 могут использоваться в различных комбинациях друг с другом, определяющих стратегии архивации (см. табл. 4.2). При выборе стратегии архивации обычно учитывают два критерия – это время, необходимое для архивации и восстановления данных. Во многих организациях стратегии архивации рассчитаны на недельный цикл.

Таблица 4.2
Стратегии архивации

№	Стратегия архивации	Необходимое время для архивации	Необходимое время для восстановления

	Описание		
1	Полная архивация	Максимальное	Минимальное
	На практике отдельно полная архивация в еженедельном цикле не используется. Однако при незначительном изменении архивируемых данных на сервере (рабочей станции), она может выполняться один раз в неделю.		
2	Полная архивация с последующей добавочной	Минимальное	Максимальное
	В понедельник выполняется обычная архивация, со вторника по пятницу - добавочная. Так как каждая из этих архиваций сбрасывает бит архива, то ежедневно архивируются только измененные файлы. Если произойдет сбой данных в пятницу, то необходимо будет восстановить обычный архив от понедельника и последовательно каждый добавочный архив со вторника по четверг.		
3	Полная архивация с последующей разностной	Промежуточное между стратегиями 1 и 2	Промежуточное между стратегиями 1 и 2
	В понедельник выполняется обычная архивация, со вторника по пят-		

ницу - разностная. Так как разностная архивация не сбрасывает бит архива, то каждый ежедневно архивируются все изменения, произошедшие с понедельника. Если произойдет сбой данных в пятни-

цу, то необходимо будет восстановить обычный архив от понедельника и последний разностный архив от четверга.

4	
Ежедневная архивация	
Зависит от количества созданных и измененных файлов за текущие сутки	
Определяется объемом восстанавливаемых данных	
Ежедневная архивация использует не атрибут файла «архивный» (бит архива), а его дату изменения. Данную стратегию целесообразно применять, если существует задача восстанавливать файлы из архива на точную дату.	

Рис. 4.8. Окно для настройки дополнительных параметров архивации

Настроить определенную стратегию архивации можно в дополнительных параметрах архивации (см. рис. 4.8), и в параметрах запланированного задания (см. рис 4.9), которые вызываются нажатием кнопок «Дополнительно» и «Расписание» в окне «Сведения о задании архивации» (см. рис. 4.7). Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 14

Рис. 4.9. Вкладка «Расписание» для настройки запланированного задания архивации

4.2.3. Восстановление данных

Главная и единственная причина создания резервных копий – это возможность восстановления данных. Успешное восстановление данных возможно, если придерживаться некоторых правил, главные из которых:

- полное документирование всех мероприятий по архивации,
- периодическое проведение тестовых восстановлений данных с архивных носителей.

В ОС Microsoft Windows 2003/XP восстанавливать папки и файлы из архива могут пользователи, входящие в группу администраторов или операторов архива. Программа Backup Windows позволяет проводить процедуру восстановления данных двумя способами: вручную и с использованием мастера. На данном занятии рассмотрим только первый способ. Настроить параметры и запустить процесс восстановления можно, перейдя на вкладку «Восстановление и управление носителем» в главном окне программы Backup (см. рис. 4.10). Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 15

Рис. 4.10. Вкладка «Восстановление и управление носителем» в окне программы Backup Windows

На этой вкладке необходимо выбрать носитель, с которого будут восстанавливаться данные. В нижней части окна можно выбрать один из следующих параметров восстановления:

- Исходное размещение – восстановление файлов и папок из архива в то же месторасположение, где они находились до архивации.
- Альтернативное размещение – восстановление файлов и папок из архива в заданную папку. Этот вариант восстановления позволяет сохранить структуру папок архивных данных.
- Одну папку – восстановление файлов и папок из архива в заданную папку без сохранения исходной структуры папок и подпапок. При этом в заданной папке будут восстановлены только файлы.

При выборе вариантов «Альтернативное размещение» или «Одну папку», необходимо задать папку, в которую будет осуществляться восстановление данных из архива. Выбрав все необходимые файлы и папки, можно запустить процесс восстановления, нажать кнопку «Восстановить». Появится диалоговое окно (см. рис. 4.11), где можно либо подтвердить восстановление, нажав кнопку «ОК», либо задать еще дополнительные параметры восстановления, нажав кнопку «Дополнительно». Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft

Рис. 4.11. Диалоговое окно, перед запуском процесса восстановления

Процесс восстановления будет отображаться в специальном окне. После его завершения выводится сводная информация об архиве в окне «Ход восстановления» (см. рис. 4.12).

Рис. 4.12. Окно «Ход восстановления» после завершения процесса восстановления

Если нажать кнопку «Отчет», то можно посмотреть информацию об ошибках и сбоях, произошедших во время процесса восстановления.

4.3. Создание отказоустойчивых томов для хранения данных

В ОС Windows Server 2003 возможно создание отказоустойчивых томов RAID-1 (зеркальный том) и RAID-5, которые поддерживаются только на динамических дисках. По умолчанию ОС Microsoft Windows 2003/XP используют традиционное базовое хранение. Для эффективности управления хранением данных базовые диски преобразуют в динамические, на которых можно создавать различные типы томов. Более подробную инфор-

мацию об управлении дисковыми хранилищами в ОС Windows Server 2003 можно узнать из источников [5, 9].

4.3.1. Работа с зеркальными томами

Зеркальный том (RAID 1) состоит из двух одинаковых копий тома, расположенных на разных физических дисках. Данные, записываемые на такой том, записываются одновременно на два диска, поэтому зеркальный том обеспечивает отказоустойчивость. Для более высокой отказоустойчивости рекомендуется использовать диски, подключенные к разным контроллерам, что обеспечит наилучшую производительность и позволит справиться с отказами как контроллера, так и диска.

В ОС Windows Server 2003 для работы с дисками существует специальная оснастка «Управление дисками», которая входит в консоль «Управление компьютером». Для создания зеркального тома необходимо сначала с помощью оснастки «Управление дисками» преобразовать тип хранения с базового в динамическое на двух подключенных физических дисках. После этого щелкните на неразмеченную область в графическом представлении диска, и в появившемся контекстном меню выберите команду «Действие» / «Все задачи» / «Создать том». Запустится мастер создания томов, который предложит сначала выбрать тип тома (см. рис. 4.13).

Рис. 4.13. Доступные типы томов в ОС Windows Server 2003

Доступные типы томов зависят от числа установленных дисков на компьютере, содержащих неразмеченные области. Для создания зеркального тома, как было сказано выше, необходимо два динамических диска имею-

щих нераспределенное место. Выбрав нужный тип тома, мастер создания томов откроет страницу, показанную на рис. 4.14, на которой следует выбрать диски для создания тома [5].

Рис. 4.14. Страница выбора дисков для добавления в зеркальный том

Выбрав диски для создания тома, следует определить еще его размер. Для этого на каждом из дисков необходимо отвести области одинаковых размеров. После выбора дисков для тома укажите в поле «Выберете размер выделяемого пространства (Мб)» максимальный размер области, доступной на каждом из выбранных дисков (он ограничен размером области на диске с минимальным размером свободного места). При изменении размера отведенного места на одном из дисков мастер соответствующим образом изменит размер места, отведенного для нового тома на другом диске. Общий размер зеркального тома равен выделенной области (в Мб), так как диски данного типа тома содержат одинаковые копии данных. После завершения работы «Мастера создания томов» будет создан зеркальный том. Для начала эксплуатации зеркального тома нужно дождаться окончания процессов его форматирования и ресинхронизации (см. рис. 4.15).

© Факультет «Информационные системы в управлении» СибАДИ П.С. Ложников, Е.М. Михайлов
http://www.isu.kasib.ru

Рис. 4.14. Список дисков в оснастке «Управление дисками»

Процесс восстановления неисправного диска зеркального тома зависит от типа неисправности. Если на диске возникли одиночные ошибки ввода-вывода, оба диска тома перейдут в состояние «Отказавшая избыточность», диск с ошибками находится в состоянии «Автономный» или «Отсутствует» (рис. 4.15) [9].

Рис. 4.15. Зеркальный том в состоянии «Отказавшая избыточность»

Устранив источник ошибок ввода-вывода, например, плохое соединение кабеля, необходимо выбрать том сбойного диска или сам диск, и в контекстном меню указать пункт «Реактивизировать том» или «Реактивизировать диск» соответственно. Повторная активизация переводит диск или том в оперативный режим. Повторная синхронизация зеркального тома выполняется автоматически.

Удалить зеркальный том можно тремя способами [5]:

- Удалить том полностью со всеми данными.
- Удалить один из дисков зеркального тома. При этом на одном из дисков остается неразмеченная область, а содержимое зеркального тома сохраняется на другом диске.
- Разделить зеркальный том. При этом остаются два диска с идентичными копиями данных.

В случае выхода из строя одного физического диска зеркального тома, можно его заменить, а потом пересоздать зеркальный том. Для этого следует сначала разделить зеркальный том, затем удалить неисправный диск. Второй исправный диск станет простым томом. После замены неисправного диска на сервере, щелкните правой кнопкой мыши на оставшемся простом томе от прежнего «зеркала» и при помощи команды «Добавить зер-Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 21

© Факультет «Информационные системы в управлении» СибАДИ П.С. Ложников, Е.М. Михайлов
http://www.isu.kasib.ru

кальный том» создайте новый зеркальный том на основе добавленного диска [9].

4.3.2. Работа с томами RAID-5

Том RAID-5 состоит как минимум из трех дисков (максимум из 32). По сравнению с зеркальными томами, он обеспечивает лучшую производительность операции чтения данных и эффективность использования диско-

вого пространства. В минимальном томе RAID-5 из трех дисков, только одна треть дискового пространства используется для обеспечения отказоустойчивости (для хранения данных четности), в отличие от зеркального тома, где этот показатель равен одной второй. Отказоустойчивость зеркальных томов и RAID-5 защищает только от одиночных сбоев одного диска!

Создается том RAID-5 аналогично зеркальному через оснастку «Управление дисками», за исключением того, что изначально требуется минимум три свободных диска. При отказе одного из дисков в томе RAID-5, данные все равно будут доступны. Общая производительность тома снизится, так как при чтении отсутствующие данные будут вычисляться из оставшихся данных и информации о четности [9].

После восстановления или замены отказавшего диска, возможно, придется воспользоваться командой «Повторить сканирование» оснастки «Управление дисками» и реактивировать том на восстановленном диске. При этом система восстановит отсутствующие данные по значениям четности и заново заполнит диск, в результате том восстановит функциональность и отказоустойчивость [5].

4.4. Лабораторная работа. Обеспечение безопасности хранения данных в ОС Microsoft Windows 2003/XP.

На этой лабораторной работе вы опробуете описанные выше способы обеспечения безопасности хранения данных в ОС Microsoft Windows 2003/XP. Упражнения выполняются на виртуальных машинах с ОС Windows Server 2003 и Windows XP Professional

4.4.1. Упражнение 1. Подготовка виртуальной машины с ОС Windows 2003 Server для выполнения лабораторной работы

Упражнение выполняется на виртуальной машине с ОС Windows Server 2003.

1. Перед запуском виртуальной машины с ОС Windows Server 2003 создайте три жестких диска емкостью по 2 Гб и подключите их (удалите устройство CD-ROM).
2. Запустите виртуальную машину с ОС Windows Server 2003.
3. Зарегистрируйтесь в системе как пользователь с правами администратора. Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft

4. Выберите «Пуск», на ярлыке «Мой компьютер» нажмите правую кнопку мыши, в контекстном меню перейдите на «Управление». В появившемся окне «Управление компьютером» выберите оснастку «Управление дисками».
5. Запустится мастер инициализации и преобразования дисков. Нажмите кнопку «Далее».
6. Появится окно «Выбор диска для инициализации», в котором будут отмечены диски, которые вы добавили (если все три, то будут доступны «Диск 1», «Диск 2» и «Диск 3»). Нажмите кнопку «Далее».
7. В следующем окне «Выбор дисков для преобразования» отметьте все доступные диски и нажмите кнопку «Далее».
8. В появившемся окне «Завершение мастера инициализации» нажмите кнопку «Готово». В оснастке «Управление дисками» убедитесь, что все три присоединенных диска находятся в состоянии «Подключен».
9. Теперь на подключенных дисках необходимо создать разделы. Правой клавишей мыши поочередно щелкайте в нераспределенную область (черного цвета) дисков, и в появившемся меню выбирайте «Создать раздел». (Если появится пункт «Создать том», то это означает, что присоединенный диск использует динамическое хранение. Правой клавишей мыши щелкните на иконку «Диск 1» и выберите в меню пункт «Преобразовать в базовый диск». Теперь выполните пункт 9 этого упражнения). Рассмотрим процесс создания раздела на примере одного диска.
10. Запустится мастер создания разделов. Нажмите кнопку «Далее».
11. В окне «Выбор типа раздела» оставьте вариант «Основной раздел» и нажмите кнопку «Далее».
12. В появившемся окне «Указание размера раздела» ничего не меняйте, оставьте предложенный размер и нажмите кнопку «Далее».
13. В следующем окне «Назначение буквы диска или пути» установите переключатель на вариант «Назначить букву диска (A-Z):» и выберите первую доступную по алфавиту букву. Нажмите кнопку «Далее».
14. Откроется окно «Форматирование раздела». По умолчанию переключатель стоит на варианте «Форматировать данный раздел следующим образом:». Выбрана файловая система «NTFS», размер кластера – «По умолчанию». Установите флажок «Быстрое форматирование» и нажмите кнопку «Далее».
15. В появившемся окне «Завершение мастера создания раздела» нажмите кнопку «Готово». Вы увидите, что область диска стала синего цвета, и «Диск 1» быстро форматируется под файловую систему NTFS. Повто-

рите пункты 9-15 этого упражнения для остальных подключенных дисков.

16. Закройте окно «Управление компьютером». С помощью проводника Windows убедитесь, что у вас четыре диска включая системный – диск C:\ Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 23

4.4.2. Упражнение 2. Работа с теневыми копиями для общих папок

В этом упражнении вы запустите и настроите поддержку теневых копий на томах ОС Windows Server 2003. Вы также восстановите из теневой копии удаленные файлы в общей папке на сервере. Упражнение выполняется на виртуальной машине с ОС Windows Server 2003.

1. На диске D:\ создайте папку «Документы» и откройте ее для общего доступа с тем же именем и разрешением «Полный доступ» для всех пользователей.
2. Выберите «Пуск» / «Мой компьютер». Нажмите правую кнопку мыши на ярлыке диска D:\, в контекстном меню перейдите на «Свойства». В появившемся окне перейдите на вкладку «Теневые копии» (рис. 4.1).
3. В списке томов выберите диск D:\ и нажмите кнопку «Параметры».
4. В выпадающем списке «Расположено на томе» выберите диск E:\, на котором будут храниться данные теневых копий. В поле максимальный размер области хранения оставьте установки по умолчанию. Нажмите кнопку «OK».
5. Нажмите кнопку «Включить». Появится диалоговое окно «Включение теневого копирования», которое проинформирует вас о том, что будут применены настройки по умолчанию и будет создана первая теневая копия. Нажмите кнопку «Да».
6. Внизу в области «Теневые копии выбранного тома» появится запись о создании первой теневой копии. Не закрывайте окно «Свойства» диска D:\
7. Откройте проводник Windows. В адресной строке введите UNC-путь к вашему серверу – \\Server01 и нажмите клавишу «Enter». Отобразятся общие ресурсы сервера.
8. Нажмите правую кнопку мыши на общей папке «Документы», в контекстном меню перейдите на «Свойства». Убедитесь, что в появившемся окне стала доступна вкладка «Предыдущие версии» (рис. 4.4). За-

кройте окно «Свойства» общей папки «Документы», нажав кнопку «ОК».

9. Создайте в папке «Документы» текстовый файл – Отчет.txt. В первой строке этого файла введите текст – Запись 1. Сохраните изменения в текстовом документе.

10. Перейдите на вкладку «Теневые копии» окна свойств диска D:\. Следующая теневая копия будет создана согласно установленного по умолчанию расписания. Для демонстрации работы теневых копий общих папок ускорим процесс их создания.

11. Нажмите кнопку «Создать» внизу вкладки «Теневые копии». Через несколько секунд в списке появится запись о новой копии с текущим временем. Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft

12. Перейдите в папку «Документы», откройте текстовый файл Отчет.txt и во второй строке этого файла введите текст – Ошибочная запись 2. Сохраните изменения в текстовом документе.

13. Теперь восстановим документ Отчет.txt на тот момент, когда в нем не было ошибочной записи. Откройте проводник Windows. В адресной строке введите UNC-путь к общей папке – \\Server01\Документы и нажмите клавишу «Enter».

14. Нажмите правой кнопкой мыши на файл Отчет.txt, в контекстном меню выберите «Свойства». Перейдите на вкладку «Предыдущие версии».

15. В поле «Версии файлов» будет доступна и выделена одна копия, которая была создана вами ранее (см. п. 11) до внесения ошибочной записи в текстовый документ. Нажмите кнопку «Восстановить».

16. Появится диалоговое окно, предупреждающее вас о том, что вы решили вернуться к предыдущей версии файла. Нажмите кнопку «Да».

17. Откройте текстовый файл Отчет.txt и убедитесь, что строка «Ошибочная запись 2» отсутствует. Закройте документ, не внося в него никаких изменений. Далее рассмотрим случай, когда требуется восстановить по ошибке удаленный файл из теневой копии. Удалите файл Отчет.txt (Можно даже удалить его минуя «Корзину». Для этого нажмите клавиши «Shift» + «Del»).

18. Откройте проводник Windows. В адресной строке введите UNC-путь к вашему серверу – \\Server01 и нажмите клавишу «Enter». Нажмите правую кнопку мыши на общей папке «Документы», в контекстном меню выберите «Свойства». На вкладке «Предыдущие версии» выберите самую позднюю по времени копию и нажмите кнопку «Показать».
19. Откроется проводник, в котором отобразится содержимое папки «Документы» на момент времени создания текущей копии. В нашем случае папка содержит лишь один файл Отчет.txt.
В реальной практике в общей папке могут быть другие файлы и вложенные папки. Вам необходимо выбрать нужный для восстановления файл и скопировать его в нужное место (можно в эту же общую папку). Если бы вы нажали кнопку «Восстановить» вместо «Просмотр» на предыдущем шаге упражнения, то произошло бы восстановление всего содержимого данной папки. Таким образом, вы бы могли перезаписать файлы, измененные после указанного на копии времени, что привело бы к нарушению целостности данных! Поэтому не рекомендуется пользоваться вариантом «Восстановить» папку из теневой копии.
20. Скопируйте файл Отчет.txt в прежнюю папку \\Server01\Документы.
Таким образом, вы восстановили удаленный файл из теневой копии.

4.4.3. Самостоятельное упражнение 1. Восстановление файлов из теневой копии на клиентском компьютере с ОС Windows XP Professional

Запустите виртуальную машину с ОС Windows XP Professional и установите сетевое подключение с сервером, на котором выполнялись предыдущие упражнения. С клиентского компьютера под управлением ОС Windows XP Professional подключитесь к общей папке \\Server01\Документы. Внесите изменения в файл Отчет.txt, создайте принудительно на сервере теневую копию тома, а затем на клиентском компьютере восстановите прежнюю версию файла. Если вкладка «Предыдущие версии» будет не доступна в свойствах файла Отчет.txt, находящегося в общей папке \\Server01\Документы, то установите специальное клиентское ПО (находится в папке %systemroot%\System32\Clients\Twclient\X86 на сервере с ОС Windows

Server 2003).

4.4.4. Упражнение 3. Выполнение архивации

В этом упражнении с помощью программы Backup вы выполните полную, а затем добавочную архивацию. Вы также научитесь создавать задания для программы архивации, которые будут выполняться по расписанию. Упражнение выполняется на виртуальной машине с ОС Windows Server 2003.

1. В папке D:\Документы, где содержится файл Отчет.txt, создайте еще два текстовых документа с произвольным содержимым, например, Планы.txt и Заказы.txt.
2. В проводнике Windows выберите режим просмотра содержимого папки D:\ Документы в виде таблицы (Меню «Вид» / «Таблица»). Обратите внимание, что в столбце «Атрибуты» у всех трех файлов установлен атрибут «архивный» (бит архива обозначается буквой «А»).
3. Выберите «Пуск» / «Программы» / «Стандартные» / «Служебные» / «Архивация данных». Программа Backup Windows первый раз запускается в режиме мастера. На первой странице мастера (см. рис. 4.5) снимите флажок «Всегда запускать в режиме мастера» и нажмите на ссылку «Расширенный режим».
4. Запустится программа архивации. Перейдите на вкладку «Архивация».
5. В меню «Задание» выберите команду «Создать».
6. Раскройте узел «Мой компьютер», диск D:\, папка «Документы». Установите флажок напротив папки «Документы».
7. Внизу, в поле «Носитель архива или имя файла» введите имя будущего архива – E:\doc-normal.bkf.
8. Нажмите кнопку «Архивировать». Откроется окно «Сведения о задании архивации». Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 26

9. В разделе «Если носитель уже содержит архивы» оставьте переключатель «Дозаписать этот архив к данным носителя».
10. Нажмите кнопку «Дополнительно». Убедитесь, что выбран тип архива «Обычный» и установите флажок «Проверка данных после архивации». Нажмите кнопку «ОК», а затем «Архивировать».
11. Откроется диалоговое окно «Ход архивации», и начнется процесс архи-

вации. По завершении создания архива нажмите кнопку «Отчет» и посмотрите отчет. В нем не должно быть ошибок архивации.

12. Закройте отчет и окно «Ход архивации». Не закрывайте программу Backup Windows.

13. Обратите внимание, что в папке D:\Документы теперь у всех файлов снят атрибут «архивный».

14. Откройте файл Планы.txt и добавьте новую строку с текущей датой. Сохраните и закройте файл. Обратите внимание, что после внесения изменений в файл атрибут «архивный» автоматически устанавливается операционной системой.

15. Вернитесь к программе Backup Windows на вкладку «Архивация».

16. В меню «Задание» выберите команду «Создать».

17. Раскройте узел «Мой компьютер», диск D:\, папка «Документы». Установите флажок напротив папки «Документы».

18. Внизу, в поле «Носитель архива или имя файла» введите имя добавочного архива – E:\doc-inc.bkf.

19. Нажмите кнопку «Архивировать». Откроется окно «Сведения о задании архивации».

20. Нажмите кнопку «Дополнительно». Выберите тип архива «добавочный» и установите флажок «Проверка данных после архивации». Нажмите кнопку «ОК».

21. Теперь кнопку «Расписание». Появится диалоговое окно, которое предложит вам сохранить заданные параметры, перед установкой архивации по расписанию. Нажмите кнопку «Да».

22. Сохраните набор ваших файлов под именем documents.bks.

23. В окне «Указание учетной записи» введите свой пароль и нажмите кнопку «ОК».

24. В появившемся окне «Параметры запланированного задания» введите имя задания – «Ежедневный добавочный архив». Затем нажмите кнопку «Свойства».

25. Откроется окно «Запланированное задание», вкладка «Расписание». В выпадающем списке «Назначить задание» выберите вариант «ежедневно» и установите время начала на три минуты вперед от текущего времени, чтобы увидеть результат выполнения задания. Нажмите кнопку «ОК».

26. Введите повторно свой пароль и нажмите кнопку «ОК».

27. В окне «Параметры запланированного задания» также нажмите «ОК». Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft

28. Перейдите на вкладку «Запланированные задания» программы архивации Backup и убедитесь, что ваше задание «Ежедневный добавочный архив» появилось в расписании (Каждый день, начиная с текущего).
29. Закройте программу Backup. Дождитесь наступления времени установленного вами на запуск задания архивации. Вы увидите как запустится по расписанию программа Backup. После ее выполнения на диске E:\ появится добавочный архив doc-inc.bkf.
30. Запустите программу Backup. В меню «Сервис» выберите «Отчет». появится окно со списком отчетов архивации. Выберите последний и откройте его.
31. Сравните полученный отчет с предыдущим. Закройте все окна программы Backup. Обратите внимание, что в папке D:\Документы опять у всех файлов снят атрибут «архивный».
32. Удалите папку «Документы» со всеми файлами.

4.4.5. Упражнение 4. Восстановление данных

В этом упражнении с помощью программы Backup вы восстановите данные ранее заархивированные. Упражнение выполняется на виртуальной машине с ОС Windows Server 2003.

1. Запустите программу Backup и перейдите на вкладку «Восстановление и управление носителем».
2. В левом окне щелкните на узел «Файлы», чтобы раскрыть его. Выберите архив doc-normal.bkf.
3. Раскройте архив doc-normal.bkf и установите флажок напротив папки «Документы». Восстановим эту папку в ее исходное размещение. По умолчанию задан такой параметр снизу в выпадающем списке «Восстановить файлы в:».
4. Нажмите кнопку «Восстановить». В диалоговом окне «Подтверждение восстановления» нажмите кнопку «ОК».
5. В окне «Проверка расположения архивного файла» также нажмите кнопку «ОК».
6. После завершения восстановления закройте окно «Ход восстановления», нажав кнопку «Закрыть». Не закрывайте программу Backup Windows.
7. Убедитесь, что папка «Документы» со всеми файлами восстановлена в

прежнее место на диск D:\. Откройте файл Планы.txt и убедитесь, что он не содержит последнюю строку текста с текущей датой.

8. Вернитесь в программу Backup на вкладку «Восстановление и управление носителем».

9. В левом окне щелкните и раскройте архив doc-inc.bkf и установите флажок напротив папки «Документы», в которой содержится один файл Планы.txt. По умолчанию программа Backup не заменяет сущест-

вующие файлы с одинаковым именем. Поэтому необходимо сделать следующую настройку.

10. В меню «Сервис» выберите пункт «Параметры» и перейдите на вкладку «Восстановление». На этой вкладке переключитесь на вариант «Заменять файл на компьютере, только если он старее» и нажмите кнопку «ОК».

11. Нажмите кнопку «Восстановить». В диалоговом окне «Подтверждение восстановления» нажмите кнопку «ОК».

12. Если появится окно «Проверка расположения архивного файла», то также нажмите кнопку «ОК».

13. После завершения восстановления закройте окно «Ход восстановления», нажав кнопку «Закрыть». Закройте программу Backup Windows.

14. Убедитесь, что восстановлена последняя версия файла Планы.txt.

4.4.6. Самостоятельное упражнение 2. Архивация и восстановление данных при использовании другой стратегии

На основе сценариев упражнений 3 и 4 выполните самостоятельно упражнение, используя стратегию полной архивации с последующей разностной. Особо обратите внимание на процедуру восстановления файлов при использовании данной стратегии.

4.4.7. Упражнение 5. Использование зеркальных томов в ОС Windows Server 2003.

В этом упражнении вы создадите на сервере с ОС Windows Server 2003 отказоустойчивый зеркальный том, искусственно сделаете сбой одного из дисков тома, а затем восстановите данные. Перед выполнением данного упражнения выполните самостоятельные упражнения 1 и 2, так как данные на диске D:\ будут утрачены.

1. На сервере временно скопируйте папку «Документы» на диск C:\.
2. Выберите «Пуск», на ярлыке «Мой компьютер» нажмите правую кнопку мыши, в контекстном меню перейдите на «Управление». В появившемся окне «Управление компьютером» выберите оснастку «Управление дисками».
3. Правой клавишей мыши щелкните в графическое представление «Диск 1» (основной раздел – синего цвета), и в появившемся меню выберите «Удалить раздел».
4. Появится диалоговое окно с предупреждением о том, что все данные на томе будут потеряны. Нажмите кнопку «Да».
5. Повторите пункты 3-4 для «Диск 2» и «Диск 3».
6. Правой клавишей мыши щелкните на значок «Диск 1», в появившемся меню выберите «Преобразовать в динамический диск».
7. В появившемся окне со списком отметьте Диск 1, Диск 2 и Диск 3. Нажмите кнопку «OK». Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 29

8. Правой клавишей мыши щелкните в графическое представление «Диск 1» (нераспределенная область – черного цвета), и в появившемся меню выберите «Создать том».
9. Запустится мастер создания тома. На первой странице нажмите кнопку «Далее».
10. На следующей странице «Выбор типа тома» выберите вариант «Зеркальный том» и нажмите кнопку «Далее».
11. Откроется окно, где следует выбрать два диска для создания зеркального тома. Справа в поле «Выбраны» уже помещен Диск 1. Слева в поле «Доступны» имеется два возможных к добавлению Диск 2 и Диск 3. Щелкните левой кнопкой мыши на Диск 2, а затем нажмите кнопку «Добавить».
12. После добавления Диска 2 отобразится общий размер тома и активируется кнопка «Далее». Нажмите на неё.
13. В следующем окне вам будет предложено назначить букву диска. Выберите первую доступную по алфавиту, начиная с «D» и нажмите «Далее».
14. Появится страница мастера «Форматирование тома». Задайте метку то-

ма «Mirror», установите флажок «Быстрое форматирование», затем нажмите кнопку «Далее».

15. На последней странице мастера создания тома нажмите кнопку «Готово».

16. Через несколько секунд будет создан зеркальный том (в графическом представлении – темно-малинового цвета), затем начнется его форматирование и ресинхронизация.

17. Скопируйте обратно папку «Документы» с диска C:\ на D:\.

18. Выключите виртуальную машину с ОС Windows Server 2003.

19. Для демонстрации отказоустойчивости зеркального тома искусственно создадим отказ одного из двух жестких дисков. Для этого в настройках конфигурации оборудования виртуальной машины удалите жесткий диск, входящий в зеркальный том (Hard Disk 2). Затем опять запустите виртуальную машину с ОС Windows Server 2003.

20. Дождитесь загрузки ОС, зарегистрируйтесь как пользователь с правами администратора.

21. С помощью проводника Windows откройте «Мой компьютер». Вы увидите, что диск D:\ доступен. Вы можете обратиться к папке «Документы», находящейся этом диске.

22. Запустите оснастку «Управление дисками». Вы увидите, что оба диска зеркального тома находятся в состоянии «Отказавшая избыточность». А один из динамических дисков тома находится в состоянии «Отсутствует».

23. Выключите виртуальную машину с ОС Windows Server 2003. В настройках конфигурации оборудования виртуальной машины добавьте обратно тот же самый диск в ее состав.

24. Запустите виртуальную машину с ОС Windows Server 2003. Дождитесь загрузки ОС и зарегистрируйтесь как пользователь с правами администратора.

25. Запустите оснастку «Управление дисками». Вы увидите, что диски зеркального тома по-прежнему находятся в состоянии «Отказавшая избыточность», однако «Диск 1» на котором установлен знак, предупреждающий о сбое, теперь «Подключен».

26. Щелкните правой кнопкой мыши на значок «Диск 1» и в появившемся

меню выберите «Реактивизировать диск».

27. Запустится процесс ресинхронизации, по окончании которого зеркальный том перейдет в состояние «Исправен»

4.4.8. Самостоятельное упражнение 3. Восстановление зеркального тома

В предыдущем упражнении вы создали искусственный сбой зеркального тома, временно удалив, а потом вернув на место один из двух дисков. Предположим, что вам не удалось бы вернуть на место тот же самый диск, который находился в зеркальном томе из-за его поломки. Выключите виртуальную машину и еще раз удалите из ее состава «Диск 1». На виртуальной машине с ОС Windows Server 2003 у вас имеется свободный не используемый «Диск 3». Самостоятельно создайте зеркальный том на исправных дисках «Диск 2» и «Диск 3». Воспользуйтесь командами «Удалить зеркало», а затем «Добавить зеркало» контекстного меню на отказавшем зеркальном томе.

4.4.9. Упражнение 5. Использование томов RAID-5 в ОС Windows Server 2003.

В этом упражнении вы создадите на сервере с ОС Windows Server 2003 отказоустойчивый том RAID-5, искусственно сделаете сбой одного из дисков тома для демонстрации отказоустойчивости.

1. Выключите виртуальную машину с ОС Windows Server 2003. В настройках конфигурации оборудования виртуальной машины верните изъятый диск (Диск 1) в ее состав (если вы выполняли самостоятельное упражнение 3). Запустите виртуальную машину.

2. Дождитесь загрузки ОС, зарегистрируйтесь как пользователь с правами администратора.

3. На сервере временно скопируйте папку «Документы» с диска D:\ на диск C:\. Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft

4. Запустите оснастку «Управление дисками». Вы увидите, что у вас появился «Диск 1», на котором установлен знак, предупреждающий о сбое в состоянии – «Инородный».

Если вы выполняли самостоятельное упражнение 3, то вами был удален зеркальный том, в который ранее входил «Диск 1». Теперь для ОС он

«инородный». Такая же ситуация возникает, когда вы переносите с другого компьютера жесткий диск, использующий динамическое хранение. Чтобы получить доступ к такому динамическому диску, необходимо щелкнуть правой кнопкой мыши на значок «инородного» диска и в появившемся контекстном меню выбрать команду «Импорт чужих дисков». После этого диск будет импортирован в текущую систему. Задав ему букву диска, можно будет получить доступ к его данным.

5. Удалите все тома находящиеся на дисках: «Диск 1», «Диск 2» и «Диск 3». Для этого поочередно щелкайте правой кнопкой мыши в графическое представление дисков и выбирайте команду «Удалить том». В итоге вы должны получить три диска с нераспределенными областями.
6. Правой клавишей мыши щелкните в графическое представление «Диск 1» и в появившемся меню выберите «Создать том».
7. Запустится мастер создания тома. На первой странице нажмите кнопку «Далее».
8. На следующей странице «Выбор типа тома» выберите вариант «Том RAID-5» и нажмите кнопку «Далее».
9. Откроется окно, где следует выбрать три диска для создания зеркального тома. Справа в поле «Выбраны» уже помещен Диск 1. Слева в поле «Доступны» имеется два возможных к добавлению Диск 2 и Диск 3. Добавьте оба диска.
10. После того как вы выберете три диска, отобразится общий размер тома RAID-5 и активируется кнопка «Далее». Нажмите на неё.
11. В следующем окне вам будет предложено назначить букву диска. Выберите первую доступную по алфавиту, начиная с «D» и нажмите «Далее».
12. Появится страница мастера «Форматирование тома». Задайте метку тома «RAID5», установите флажок «Быстрое форматирование», затем нажмите кнопку «Далее».
13. На последней странице мастера создания тома нажмите кнопку «Готово».
14. Через несколько секунд будет создан том RAID-5 (в графическом представлении – цвета «морской волны»), затем начнется его форматирование и ресинхронизация.
15. Скопируйте обратно папку «Документы» с диска C:\ на D:\.
16. Выключите виртуальную машину с ОС Windows Server 2003.
17. Для демонстрации отказоустойчивости тома RAID-5 аналогично, как и в предыдущем упражнении, удалите один жесткий диск, входящий в Тема

том RAID-5. Затем опять запустите виртуальную машину с ОС Windows Server 2003.

18. Дождитесь загрузки ОС, зарегистрируйтесь как пользователь с правами администратора.

19. С помощью проводника Windows откройте «Мой компьютер». Вы увидите, что диск D:\ доступен, и можно обратиться к папке «Документы», находящейся этом диске.

20. Запустите оснастку «Управление дисками». Вы увидите, что диски тома RAID-5 находятся в состоянии «Отказавшая избыточность».

Если вышедший из строя диск будет утрачен, то том RAID-5 необходимо будет пересоздавать. Без переноса данных добавить новый диск вместо отказавшего в томе RAID-5 нельзя. Вы можете вернуть отказавший диск и реактивизировать том RAID-5.

4.5. Закрепление материала

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

1. Для политики безопасности организации использование технологии теневого копирования данных обеспечивает:

a) целостность;

b) доступность;

c) конфиденциальность.

2. Отметьте правильные утверждения, касающиеся применения технологии теневого копирования томов:

a) Восстанавливать удаленные файлы из теневой копии могут только пользователи с правами администратора;

b) Создавать теневые копии можно только на томах с файловой системой NTFS;

c) С помощью оснастки «Общие ресурсы» консоли «Управление компьютером» можно отметить отдельные общие папки для которых будет выполняться теневое копирование;

d) Для хранения теневых копий требуется не менее 100 Мб свободного места на выбранном томе.

3. Какие типы архивов поддерживаются программой Backup Windows?

4. Вам необходимо провести резервное копирование файлов с помощью программы Bakup, но при этом вы не хотите изменять состояние бита архива выбранных для архивации файлов. Какой тип архива необходимо выбрать для решения этой задачи? Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 33

5. Вам необходимо создать программный RAID на файловом сервере под управлением ОС Windows Server 2003, чтобы обеспечить отказоустойчивость данных. Пользователи, обращаясь к ресурсам данного файлового сервера чаще выполняют операции чтения, и гораздо реже – записи. Какой при этом тип RAID целесообразно выбрать?

6. Отметьте правильные утверждения, касающиеся отказоустойчивых томов RAID:

a) Зеркальные тома используют МЕНЬШЕ системной памяти по сравнению с томами RAID-5;

b) Зеркальные тома используют БОЛЬШЕ системной памяти по сравнению с томами RAID-5;

c) У зеркальных томов выделяется БОЛЬШЕ дискового пространства для обеспечения отказоустойчивости по сравнению с томами RAID-5;

d) У зеркальных томов выделяется МЕНЬШЕ дискового пространства для обеспечения отказоустойчивости по сравнению с томами RAID-5.

4.6. Резюме

В ОС Microsoft Windows 2003/XP имеются различные решения для обеспечения безопасности хранения данных, правильное использование и настройка которых позволяет администраторам решать большой спектр поставленных задач в этой области.

Включение теневого копирования томов обеспечивает пользователям доступ к копиям файлов в общих папках на сервере, которые были случай-

но повреждены или удалены по ошибке. Данная технология позволяет максимально быстро восстанавливать потерянные данные.

Архивация обеспечивает наивысшую степень отказоустойчивости по сравнению со всеми другими технологиями хранения данных, обеспечивающих отказоустойчивость. В составе ОС Microsoft Windows 2003/XP есть штатная программа Backup, обеспечивающая основные функции архивации.

Серверная ОС Windows Server 2003 позволяет создавать отказоустойчивые дисковые хранилища. При использовании динамического хранения данных в этой ОС, можно создавать зеркальные тома, состоящие из двух дисков с идентичными копиями данных, а также тома RAID-5 с контролем четности, в которых данные распределены порциями по нескольким дискам. Отказ одного из дисков таких отказоустойчивых томов не приводит к потере данных хранящихся на томе.

4.7. Список используемых источников

1. Microsoft Windows XP Professional. Учебный курс MCSA/MCSE / Пер. с англ. –2-е изд., испр. – М.: Русская редакция, 2003. – 1008 с.

2. Ауберт Майкл. Shadow Copies of Shared Folders / Пер. с англ. Цой А. Тема занятия: Обеспечение безопасности хранения данных в ОС Microsoft 34

© Факультет «Информационные системы в управлении» СибАДИ П.С. Ложников, Е.М. Михайлов

http://www.isu.kasib.ru

(http://www.networkdoc.ru/trainers2000/win2003/print.html?article06.html)

3. Восстановление файлов и папок с помощью программы «Архивация данных» в

Windows XP/ База знаний Microsoft: статья № 309340

(http://support.microsoft.com/kb/309340/)

4. Галатенко В.А. Основы информационной безопасности. – М.: Изд-во ИНТУИТ.ру, 2005. – 208 с.

5. Закер Крейг. Официальный учебный курс Microsoft: Управление и поддержка Microsoft Windows Server 2003 (70-290) / К. Закер; Пер. с англ. – М.: ЭКОМ; БИНОМ.Лаборатория знаний, 2006. – 447 с.

6. Использование программы «Архивация данных» в Microsoft Windows XP / База знаний Microsoft: статья № 308422

(http://support.microsoft.com/kb/308422/)

7. Новые возможности управления хранилищами / Официальный сайт Microsoft

(http://www.microsoft.com/Rus/WindowsServer2003/evaluation/overview/technologies/s

torage.mspx)
8. Резервное копирование и восстановление информации / Курс «Системный администратор компьютерной сети»
(http://www.xnets.ru/plugins/content/content.php?content.119.1)
9. Холме Дэн, Томас Орин. Управление и поддержка Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Пер. с англ. – М.: Русская редакция, 2004. – 448 с.