

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Белгородский государственный технологический
университет им. В.Г. Шухова

Е. А. Федотов

**АДМИНИСТРИРОВАНИЕ ПРОГРАММНЫХ И
ИНФОРМАЦИОННЫХ СИСТЕМ**

Утверждено ученым советом университета в качестве
учебного пособия для студентов специальности
230105 – Программное обеспечение вычислительной техники и
автоматизированных систем

Белгород
2012

УДК004.45 (07)
ББК 32.973.26-018.2 я7
Ф 34

Рецензенты: канд. техн. наук, доц. *В.Г. Синюк*
канд. техн. наук, доц. *В.М. Михелев*

Федотов Е. А.

Ф34 Администрирование программных и информационных систем:
учебное пособие / Е.А. Федотов. – Белгород: Изд-во БГТУ, 2012.
– 136 с.

Это учебное пособие посвящено администрированию программных и информационных систем. В нем рассмотрены все основные аспекты виртуализации операционных систем и администрирования Windows Server 2003.

Учебное пособие предназначено для студентов специальности 230105 – Программное обеспечение вычислительной техники и автоматизированных систем.

Данное издание публикуется в авторской редакции.

УДК 004.45 (07)
ББК 32.973.26-018.2 я7

© Белгородский государственный технологический
университет им. В.Г. Шухова, 2012

Оглавление

<u>Введение.....</u>	<u>6</u>
<u>1. Установка, настройка и администрирование Windows Server 2003 с использованием виртуальных машин.....</u>	<u>7</u>
Виртуализация операционных систем.....	7
Установка виртуальной машины на примере MS Virtual PC.....	10
Установка операционной системы в виртуальной машине.....	15
Настройка Windows Server 2003.....	18
Active Directory.....	21
Консоли MMC.....	24
Службы терминалов.....	27
Windows Messenger.....	30
<u>2. Создание сценариев с помощью Microsoft Windows Script Host.....</u>	<u>34</u>
Способы выполнения сценариев Windows.....	34
Протокол LDAP.....	38
Определение переменных и обработка ошибок.....	39
<u>3. Учетные записи пользователей.....</u>	<u>41</u>
Планирование учетных записей пользователей.....	42
Создание объектов пользователей	45
Управление учетными записями пользователей	48
Создание нескольких объектов пользователей.....	51
Импорт объектов пользователей при помощи CSVDE.....	52
Использование средств командной строки Active Directory.....	53

Управление профилями пользователей.....	59
Политика паролей.....	61
Политика блокировки учетной записи.....	63
Политики аудита.....	64
Управление проверкой подлинности пользователей.....	66
4. Учетные записи групп. Групповые политики.....	68
Понятие типа группы и области действия.....	68
Специальные группы.....	70
Создание объектов групп и управление ими.....	71
Автоматизация управления учетными записями групп	72
Управление группами с помощью сценариев.....	74
5. Учетные записи компьютеров.....	81
Создание учетных записей компьютеров.....	81
Присоединение компьютера к домену.....	83
Управление разрешениями для объекта компьютера.....	86
Настройка свойств объекта компьютера.....	87
Поиск и подключение к объектам в Active Directory.....	87
Устранение неполадок с учетными записями компьютеров.....	88
Выявление проблем с учетными записями компьютеров.....	91
Анатомия объекта computer.....	92
6. Файлы и папки.....	94
Открытие общего доступа к папке.....	94
Управление общей папкой.....	95

<u>Настройка разрешений доступа к общему ресурсу.....</u>	<u>96</u>
<u>Управление сеансами пользователей и открытыми файлами.....</u>	<u>98</u>
<u>Настройка разрешений файловой системы.....</u>	<u>98</u>
<u>Наследование.....</u>	<u>102</u>
<u>Действующие разрешения.....</u>	<u>104</u>
<u>Права владения ресурсом.....</u>	<u>105</u>
<u>Аудит доступа к файловой системе.....</u>	<u>107</u>
<u>Администрирование служб IIS.....</u>	<u>111</u>
<u>7. Архивация и восстановление данных.....</u>	<u>118</u>
<u>Введение в архивацию.....</u>	<u>118</u>
<u>Стратегии архивирования.....</u>	<u>120</u>
<u>Дополнительные возможности архивации и восстановления.....</u>	<u>124</u>
<u>Планирование заданий архивации.....</u>	<u>129</u>
<u>Теневые копии общих папок.....</u>	<u>130</u>
<u>Заключение.....</u>	<u>134</u>
<u>Библиографический список.....</u>	<u>135</u>

Введение

Операционная система Windows Server 2003 является логическим результатом эволюции Windows 2000 Server и Windows XP. При ее разработке особое внимание уделялось сетевой безопасности, надежности, производительности и устойчивости к сетевым атакам.

Операционные системы семейства Microsoft Windows 2003 на сегодняшний день относятся к числу наиболее совершенных и стабильных программных продуктов, получивших широкое признание и распространение в сфере информационно-коммуникационных технологий. Это одна из самых эффективных платформ для построения инфраструктуры сетевых приложений, сетей и веб-служб: от рабочей группы до центра обработки данных.

Windows Server 2003 включает множество инструментов и средств конфигурирования, настройки и администрирования операционной среды. Windows Server 2003 позволяет создавать безопасную инфраструктуру, которая обеспечивает мощную платформу для приложений с возможностью быстрого построения сетевых решений.

Данное пособие предназначено для студентов, заинтересованных в подробном изучении серверных операционных систем и их виртуализации. Все материалы учебного пособия подготовлены преимущественно для студентов пятого курса специальности «Программное обеспечение вычислительной техники и автоматизированных систем», но также будет полезно студентам других специальностей, желающим поближе познакомиться с серверными операционными системами и виртуализацией серверов.

1. Установка, настройка и администрирование Windows Server 2003 с использованием виртуальных машин

Виртуализация операционных систем

Виртуализация операционных систем представляет собой процесс создания так называемой виртуального компьютера на физическом (хостовом) компьютере, в который устанавливается своя собственная операционная система. На одном хостовом компьютере виртуальных машин может быть несколько со своими виртуальными аппаратными компонентами такими как оперативную память, процессоры, винчестеры, сетевые адаптеры и т.д. Эти ресурсы используются виртуальной машиной за счет физических ресурсов аппаратного обеспечения хостового компьютера. Такая модель организации вычислительных систем впервые появилась в 70-х годах 20 века в мэйнфреймах корпорации IBM System 360/370, когда требовалось сохранить предыдущие версии экземпляров операционных систем. Но лишь в настоящее время эта технология обрела новый смысл в кластерных системах и серверах. Виртуальная и хостовая операционные системы работают одновременно, обмениваются данными и участвуют в сетевом взаимодействии с внешней, по отношению к хостовому компьютеру, сетью [6].

Одновременный запуск нескольких операционных систем на одном компьютере имеет следующие преимущества:

1. Можно работать в виртуальной машине с устаревшими приложениями, которые не работают в хостовой операционной системе компьютера (например, если хостовая ОС - Windows 7, то можно установить Windows 98, в которой работает старая игра или программа, и запускать виртуальную ОС в любое время, без необходимости перезагружать компьютер).

2. Можно создавать защищенные пользовательские окружения для работы с сетью. Вирусы и другое вредоносное программное обеспечение смогут лишь повредить гостевую операционную систему виртуальной машины, не затронув реальную ОС.

3. Появляются практически неограниченные возможности для экспериментов с операционными системами. Можно устанавливать любые программы, которые потенциально могут повредить операционную систему, экспериментировать с настройками реестра и т.д., без вреда для реальной ОС.

4. Можно разрабатывать и тестировать программное обеспечение в различных операционных системах и их версиях (например, может быть установлено несколько одинаковых операционных систем с различными версиями Internet Explorer, что очень удобно, если разрабатывается какой-нибудь тулбар под этот браузер).

5. Появляются новые возможности обучения работе с новыми операционными системами и программами (например, если пользователю знает только Windows XP, можно установить несколько виртуальных машин с различными операционными системами и запускать их и учиться работать с ними, когда требуется).

Кроме вышеперечисленных преимуществ каждый может сам придумать, для каких целей ему нужна виртуальная машина. Можно установить нескольких хостовых операционных систем на один компьютер с их отдельной загрузкой, но целесообразнее установить виртуальные машины.

Преимущества использования виртуальных машин следующие:

1. Одновременная работа в нескольких операционных системах, возможность осуществлять сетевое взаимодействие между ними.

2. Возможность сделать резервирование текущего состояния системы (простым копированием ряда файлов связанных с виртуальной системой) и содержимого дисков одним щелчком мыши, и затем в течение достаточно короткого интервала времени вернуться в требуемое состояние.

3. Можно иметь на одном компьютере практически неограниченное число виртуальных машин с различными операционными системами и их состояниями для технической поддержки. Можно установить несколько экземпляров операционных систем для того, чтобы персонал службы технической поддержки, запуская нужную конфигурацию операционной системы, мог обеспечивать разрешение проблем пользователей в максимально сжатые сроки.

4. Нет необходимости перезагружать компьютер для переключения в другую операционную систему.

5. Контроль качества программного обеспечения и запуск приложений в изолированной виртуальной среде, где не страшно повреждение системы.

6. Нет необходимости в приобретении новых компьютеров для целей обучения пользованию различными операционными системами и приложениями.

Тем не менее, несмотря на перечисленные преимущества, виртуальные машины имеют и недостатки:

1. Требуется наличие значительных аппаратных ресурсов для должной работы нескольких операционных систем одновременно.

2. Операционная система в виртуальной машине работает медленнее по сравнению с хостовой. Но в последнее время показатели производительности гостевых систем приблизились к показателям физических ОС, и вскоре, за счет улучшения технологий реализации виртуальных машин, производительность гостевых систем практически будет равна реальным.

3. Существуют способы определения запущена ли в виртуальной машине программа. Распространители вредоносного программного обеспечения в курсе этих способов и в последнее время включают в свои программы функции обнаружения факта запуска в виртуальной машине, но при этом никакого ущерба вредоносное ПО гостевой системе не причиняет.

4. Различные платформы виртуализации пока не поддерживают полную виртуализацию всего аппаратного обеспечения и интерфейсов. В последнее время количество поддерживаемого аппаратного обеспечения стремительно растет у всех производителей платформ виртуализации.

Все перечисленные недостатки виртуальных машин разрешимы и, по сравнению с большим списком их достоинств, являются не столь существенными. Именно поэтому, технологии виртуализации и виртуальных машин развиваются взрывными темпами, а пользователи находят им все новые и новые применения.

В настоящее время на рынке платформ виртуализации присутствуют несколько лидирующих компаний: VMware, Microsoft, XenSource, Parallels, SWsoft, Virtual Iron и другие. У платформы каждого из производителей есть свои неоспоримые достоинства и недостатки, однако, что касается пользовательских (настольных) систем виртуализации для хостовых систем Windows, лидера всего два: компании VMware и Microsoft.

Для настольных систем компании VMware и Microsoft предлагают пользователям два продукта: VMware Workstation и Microsoft Virtual PC. Эти два продукта приблизительно равны, однако VMware Workstation, хоть и превосходящий несколько Microsoft Virtual PC по возможностям, является платным и ориентирован прежде всего на IT-профессионалов. Поэтому для настольных компьютеров большего всего подходит бесплатная платформа Virtual PC, тем более, что

поскольку производителем платформы является сама компания Microsoft, то поддержка операционных систем Windows является более полной [6].

Установка виртуальной машины на примере MS Virtual PC

Microsoft Virtual PC представляет собой программный пакет виртуализации для операционных систем семейства Windows, который позволяет эмулировать на одном компьютере работу сразу нескольких виртуальных машин. Каждая из таких машин может находиться под управлением своей собственной операционной системы (Windows любой версии, Netware, Linux, Solaris и т.д.), выполнять уникальную задачу, иметь собственную конфигурацию и т.д.

Продукт Virtual PC был создан компанией [Connectix](#) в 1997 году для операционной системы Mac OS на платформе [PowerPC Macintosh](#). В 2001 году была выпущена версия 4.0 для ОС [Windows](#). Connectix поставляла Virtual PC с различными гостевыми ОС, включая [Linux](#) и [OS/2](#). В феврале 2003 года права на продукты Virtual PC и Virtual Server были куплены компанией [Майкрософт](#). В июле 2006 года Майкрософт выпустила Windows-версию пакета для бесплатного использования.

Продукт Virtual PC предназначен для запуска одной или нескольких гостевых операционных систем на настольных системах, прост в использовании и ориентирован на неискушенных в компьютерных технологиях пользователей.

В новой версии продукта Virtual PC появились следующие основные возможности:

1. Оптимизация платформы под Windows Vista. На платформе Virtual PC 2004 также можно было установить Windows Vista, однако в новой версии продукта эта система работает гораздо быстрее и стабильней.

2. Увеличение быстродействия за счет использования улучшений, введенных в серверной платформе виртуализации Microsoft Virtual Server 2005 R2.

3. Поддержка 64-битных хостовых операционных систем Windows.

4. Поддержка звуковых устройств в гостевых системах Windows Vista.

Скачать последнюю версию программы Microsoft Virtual PC можно бесплатно на [официальной странице продукта](#) компании Microsoft. После запуска программы MS Virtual PC появляется New Virtual Machine Wizard - мастер создания новой виртуальной машины

(рис. 1.1.). Чтобы приступить к созданию виртуальной машины, нажимаем «Next».

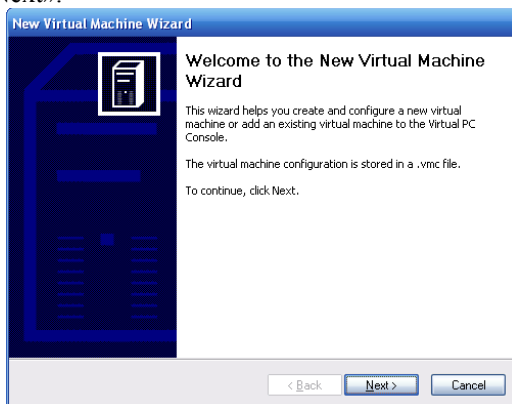


Рис. 1.1. Начальный этап создания виртуальной машины

В появившемся окне следует выбрать один из трех вариантов:

1. «Create a virtual machine» - создание новой виртуальной машины;
2. «Use default settings to create a virtual machine» - создание новой виртуальной машины с настройками по умолчанию;
3. «Add an existing virtual machine» - добавление существующей виртуальной машины (рис. 1.2.).

Для перехода к следующему шагу – «Next».

На следующем шаге следует указать место расположения и имя файла с настройками виртуальной машины (рис. 1.3.).

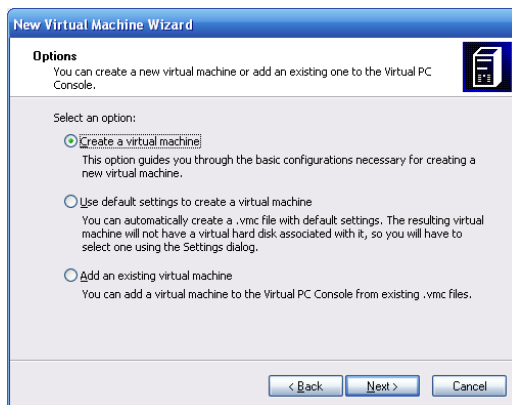


Рис. 1.2. Выбор варианта создания виртуальной машины

На диске, на котором будет храниться файл, должно быть достаточно места для установки гостевой ОС. Рекомендуется хранить файл с настройками виртуальной машины и виртуальный диск в одной директории.

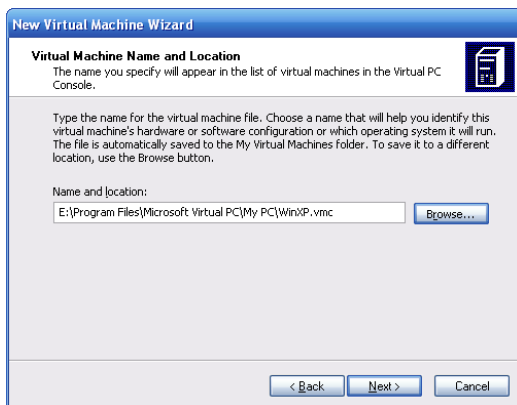


Рис. 1.3. Назначение места расположения и имени файла с конфигурацией виртуальной машины

Выбор типа гостевой операционной системы считается важным этапом, поскольку производительность системы напрямую зависит от типа гостевой ОС. Необходимо выбрать пункт «Other», если устанавливаемой ОС нет в списке «Operating system» (рис. 1.4.).

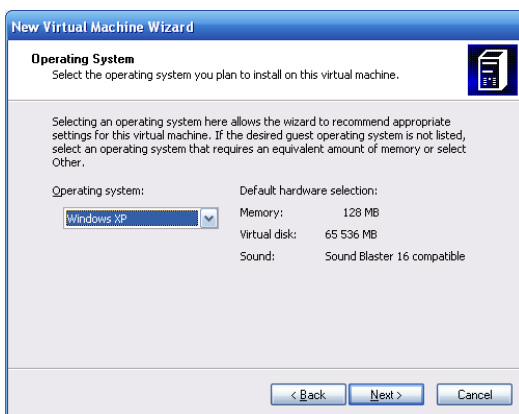


Рис. 1.4. Выбор типа гостевой операционной системы

Также можно выбрать объём оперативной памяти, который будет выделен гостевой системе. Доступны два варианта (рис. 1.5.):

1. «Using the recommended RAM» - память будет выделена по умолчанию.

2. «Adjusting the RAM» - необходимо вручную установить объём выделенной оперативной памяти с учетом минимальных требований устанавливаемой системы к объему RAM и а также объема физической памяти виртуальной машины.

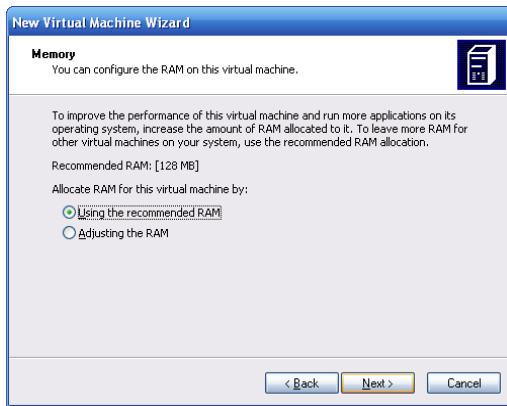


Рис. 1.5. Выбор объёма оперативной памяти

Далее необходимо выбрать, использовать ли уже имеющийся виртуальный жесткий диск («An existing virtual hard disk») или создать новый («A new virtual hard disk») (рис. 1.6.).

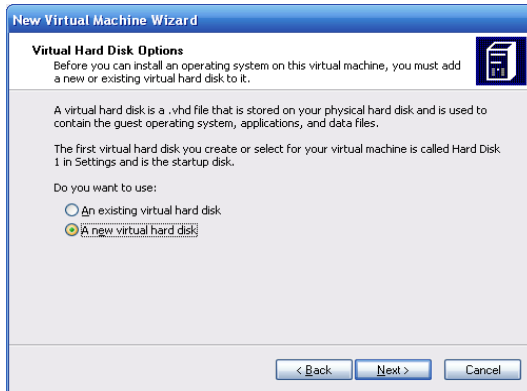


Рис. 1.6. Опции виртуального жёсткого диска

Следующий этап состоит в задании размера виртуального жесткого диска (рис. 1.7.). По умолчанию предлагается создать диск объемом 65536 Мб. Этой величиной определяется максимальный объем диска виртуальной машины, а сам файл будет расти по мере заполнения диска в виртуальной машине.

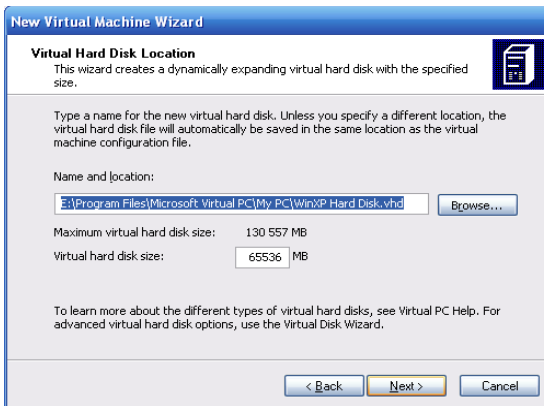


Рис. 1.7. Выбор размера виртуального жесткого диска

На завершающем этапе проверяем атрибуты виртуальной машины и, нажимаем «Finish» (рис. 1.8.). Виртуальная машина создана.

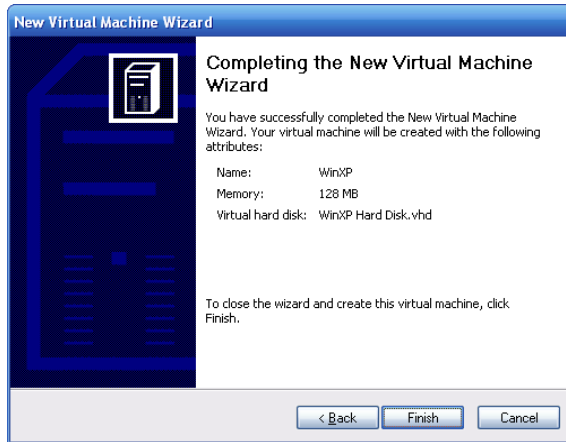


Рис. 1.8. Завершающий этап создания виртуальной машины

После нажатия кнопки «Finish» новая виртуальная машина появится в окне Virtual PC Console (рис. 1.9.):

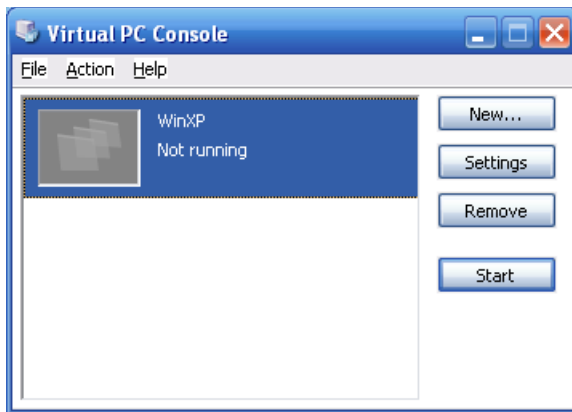


Рис. 1.9. Окно MS Virtual PC

Установка операционной системы в виртуальной машине

В главном окне программы, «Virtual PC Console», нажимаем кнопку «Start». Начнется загрузка виртуальной машины.

Далее необходимо определиться с расположением дистрибутива гостевой операционной системы. Возможные варианты. Если

дистрибутив находится на загрузочном CD или DVD диске, вставьте его в привод, так как с него по умолчанию пытается загрузиться виртуальная машина, после этого нажмите «Enter». Если дистрибутив операционной системы в виде загрузочного образа ISO, откройте меню CD консоли виртуальной машины, выберите пункт «Capture ISO Image» и укажите путь к образу. После этого начнется загрузка операционной системы.

Установка гостевой ОС производится аналогично установке на физическую машину. Виртуальная машина как бы «поглощает» указатель мыши, позволяя работать только внутри гостевой системы. Для выхода из режима захвата указателя мыши - правый Alt.

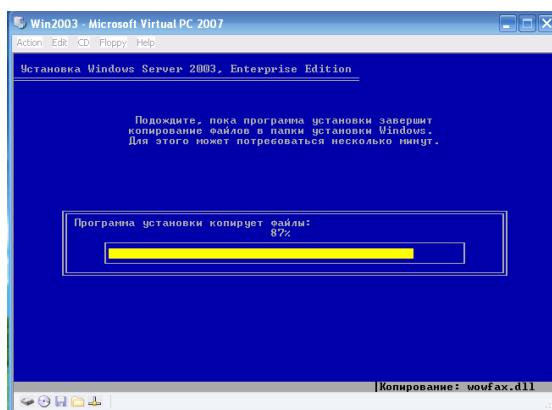


Рис. 1.10. Установка Windows Server 2003

Розничная и пробная версии Windows Server 2003 требуют активации. Такие массовые программы лицензирования, как Open License, Select License или Enterprise Agreement не требуют активации. Процедуру активации достаточно выполнить однократно. Для того чтобы начать активацию, щелкните Пуск\Все программы\Активация Windows или подкачку на системной панели. Далее необходимо следовать инструкциям Мастера активации. Для активации через интернет необходимо чтобы компьютер был подключен к сети. При отсутствии доступа в интернет можно активировать Windows по телефону.

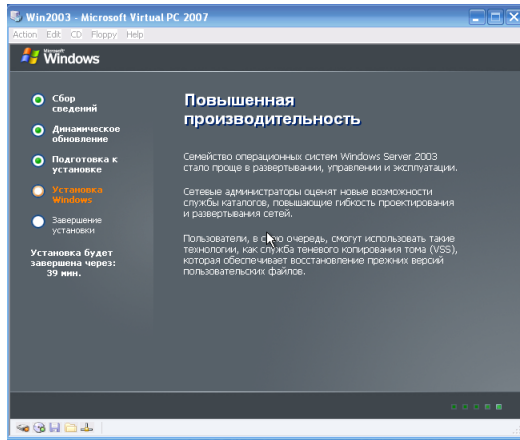


Рис. 1.11. Процесс установки ОС

Семейство Windows Server 2003 включает в себя четыре редакции операционных систем [1, 5, 9].

Windows Server 2003 Web Edition. Предназначена для веб-хостинга и поддержки XML веб-служб в небольших организациях и поддерживает 2 Гб ОЗУ и 2 центральных процессора. Эта редакция поддерживает неограниченное количество анонимных Web-соединений и 10 входящих соединений блока серверных сообщений.

Windows Server 2003 Standard Edition. Представляет собой многофункциональный сервер, предоставляющий службы каталогов, файлов, печати, приложений, мультимедийные и Web-службы для небольших и средних предприятий. Эта редакция поддерживает до 4 Гб ОЗУ и четырехпроцессорную SMP-обработку.

Windows Server 2003 Enterprise Edition. Представляет собой мощную серверную платформу для средних и крупных предприятий. Эта редакция поддерживает восемь процессоров, 32 Гб ОЗУ, восьмиузловую кластеризацию, совместимость с 64-разрядными компьютерами на базе Intel Itanium, что позволяет поддерживать уже 64 Гб ОЗУ и восьмипроцессорную SMP-обработку. Кроме того добавлена поддержка служб MMS (Microsoft Metadirectory Services), позволяющих объединять каталоги, БД и файлы со службой каталогов Active Directory. Поддерживается функция «горячего» добавления памяти.

Windows Server 2003 Datacenter Edition. Редакция доступна только в качестве OEM-версии, предлагаемой в комплекте с серверами высокого класса, и поддерживает практически неограниченную

масштабируемость: для 32-разрядных платформ — 32-процессорная SMP-обработка и 64 Гб ОЗУ, для 64-разрядных — 64-процессорная SMP-обработка и 512 Гб ОЗУ.

Все редакции поддерживают одни и те же базовые функции и средства администрирования. В редакции Windows Server 2003 Web Edition нет Active Directory, поэтому сервер, работающий под управлением этой редакции, нельзя сделать контроллером домена.

Настройка Windows Server 2003

После установки и активации Windows можно настроить сервер при помощи страницы *Управление данным сервером (Manage Your Server)*, показанной на рис. 1.12. Эта страница запускается автоматически после входа пользователя в систему. Также эту программу можно запустить в любое время, выбрав одноименную команду из меню Пуск/Администрирование. Эта страница упрощает установку некоторых служб, инструментов и конфигураций в зависимости от роли сервера.

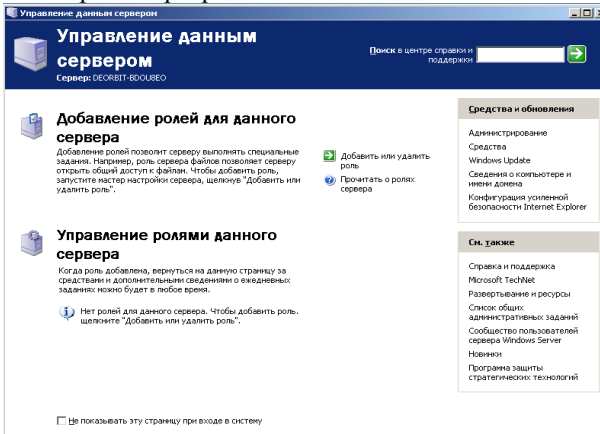


Рис. 1.12. Управление данным сервером

После нажатия на гиперссылку *Добавить или удалить роль* откроется окно *Мастер настройки сервера*. Если установить переключатель *Типовая настройка для первого сервера*, мастер сделает сервер контроллером нового домена, установит службы Active Directory и при необходимости службы DNS, DHCP и RRAS.

Если установить переключатель *Особая конфигурация*, можно выполнить настройку сервера, добавляя новые роли или удаляя роли,

ставшие ненужными. Стандартные роли, для выполнения которых можно сконфигурировать сервер следующие:

Файловый сервер. Обеспечивает централизованный доступ к файлам и каталогам для пользователей, отделов и организации в целом. Выбор этой роли позволяет управлять пользовательским дисковым пространством путем включения и настройки средств управления дисковыми квотами и ускорить поиск в файловой системе за счет активизации *Службы индексирования*.

Сервер печати. Обеспечивает централизованное управление печатающими устройствами. Предоставляет клиентским компьютерам доступ к общим принтерам и их драйверам. Если выбрать этот вариант, запустится *Мастер установки принтеров*, позволяющий установить принтеры и соответствующие драйверы. Кроме того, мастер устанавливает службы IIS 6.0, настраивает протокол печати IPP и Web-средства управления принтерами.

Сервер приложений. Предоставляет компоненты инфраструктуры, которые требуются для поддержки размещения Web приложений. Эта роль устанавливает и настраивает IIS 6.0, ASP.NET и COM+.

Почтовый сервер. Предоставляет пользователям полнофункциональный сервис по доставке и управлению почтой. Устанавливает POP3 и SMTP, чтобы сервер мог выступать в роли почтового сервера для клиентов POP3.

Сервер терминалов. Позволяет множеству пользователей с помощью клиентского ПО *Службы терминалов* или *Дистанционное управление рабочим столом* подключаться к приложениям и ресурсам сервера, например принтерам или дисковому пространству, как если бы эти ресурсы были установлены на их компьютерах.

Сервер удаленного доступа или VPN-сервер. Обеспечивает маршрутизацию по нескольким протоколам и службы удаленного доступа для коммутируемых, локальных и глобальных вычислительных сетей. *Виртуальная частная сеть* обеспечивает безопасное соединение пользователя с удаленными узлами через стандартные Интернет-соединения.

Контроллер домена Active Directory. Предоставляет службы каталогов клиентам сети. Этот вариант позволяет создать контроллер нового или существующего домена и установить DNS.

DNS-сервер. Обеспечивает разрешение имен узлов: DNS-имена преобразуются в IP-адреса (прямой поиск) и обратно (обратный поиск).

ДНСП-сервер. Предоставляет службы автоматического выделения IP-адресов клиентам, настроенным на динамическое получение IP-адресов.

Сервер потоков мультимедиа. Предоставляет службы WMS, которые позволяют серверу передавать потоки мультимедийных данных в интрасети или через Интернет. Содержимое может храниться и предоставляться по запросу или в реальном времени. Если выбрать этот вариант, устанавливается сервер WMS.

WINS-сервер. Обеспечивает разрешение имен компьютеров путем преобразования имен NetBIOS в IP-адреса. Устанавливать службу WINS не требуется, если вы не поддерживаете старые ОС, например Windows 95 или NT. Такие ОС, как Windows 2000 и XP не требуют WINS, хотя старым приложениям, работающим на этих платформах, может понадобиться разрешать имена NetBIOS. Если выбрать этот вариант, устанавливается сервер WINS.

Выбираем *Типовая настройка для первого сервера*. В поле *Имя домена в Active Directory* указывается имя домена (например povtas.ru). Убедимся, что в поле *NetBIOS-имя домена* указано POVITAS, и щелкнем *Далее*. Окно *Сводка выбранных параметров* должно соответствовать показанному на рис. 1.13.

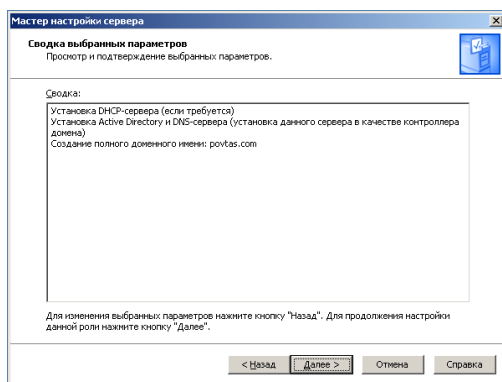


Рис. 1.13. Окно *Сводка выбранных параметров* мастера настройки сервера

Мастер напомнит, что система будет перезагружена, и попросит закрыть все открытые программы. Щелкните *Да*. После перезагрузки войдите в систему как *Администратор*. Мастер настройки сервера резюмирует установку (рис. 1.14.). Щелкните *Далее*, а затем *Готово*.

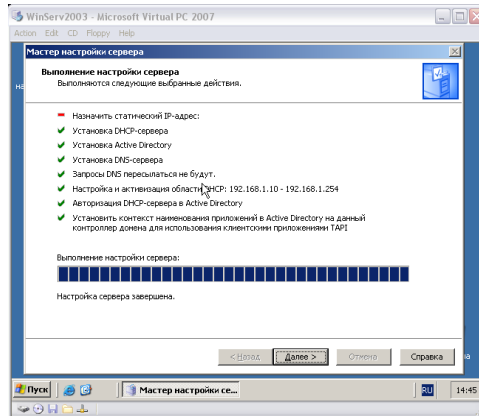


Рис. 1.14. Мастер настройки сервера на завершающем этапе

Откройте консоль *Active Directory — пользователи и компьютеры*. Убедитесь, что домен povtas.com создан: раскройте его и найдите учетную запись компьютера для Server01 в организационном подразделении (ОП) *Контроллеры домена* (рис. 1.15.).

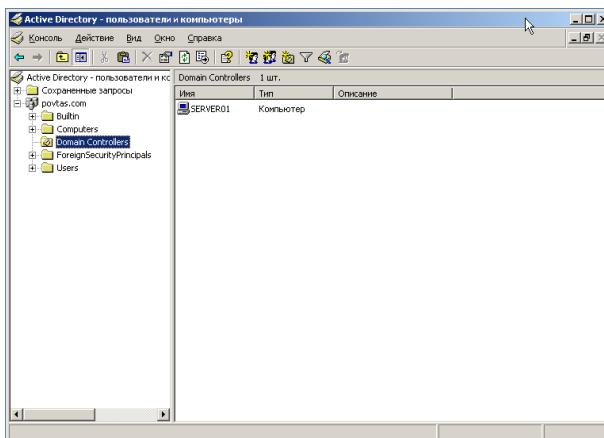


Рис. 1.15. Консоль *Active Directory – пользователи и компьютеры*

Active Directory

Сети Microsoft Windows поддерживают две модели служб каталогов: рабочие группы и домены [1, 9, 10].

Рабочая группа - логическое объединение сетевых компьютеров, которые совместно используют такие общие ресурсы, как файлы,

папки и принтеры. Рабочую группу также называют *одноранговой сетью*, т.к. все компьютеры в ней могут использовать общие ресурсы на равных условиях, т. е. без выделенного сервера.

Домен - логическое объединение компьютеров в сети, которые совместно используют центральную базу данных каталога. *База данных каталога* содержит учетные записи пользователя и информацию о политиках безопасности для домена. Эту базу данных называют каталогом, и она представляет собой часть базы данных службы Active Directory — службы каталогов Windows 2003.

Домен преобладает в корпоративных сетях. Служба Active Directory играет роль хранилища идентификационных данных, являясь единым справочником домена. Active Directory включает журналы транзакций и системные ресурсы, содержащие сценарии входа в систему, сведения о групповой политике, а также службы, поддерживающие и использующие БД, включая протокол LDAP (Lightweight Directory Access Protocol), протокол безопасности Kerberos, процессы репликации и службу FRS (File Replication Service). БД и ее службы устанавливаются на один или несколько контроллеров домена.

Домен — это основная административная единица службы каталогов. Тем не менее, предприятие может включить в свой каталог более одного домена. Несколько доменов, совместно использующих общее пространство имен DNS, образуют логические структуры, называемые *деревьями*. Например, домены povtas.com, pv-1.povtas.com и pv-2.povtas.com совместно используют непрерывное пространство имен DNS и образуют дерево.

Домены Active Directory с разными корневыми доменами образуют несколько деревьев. Они объединяются в самую большую структуру Active Directory — *лес*. Лес Active Directory содержит все домены в рамках службы каталогов. Лес может состоять из нескольких доменов в нескольких деревьях или только из одного домена. Когда доменов несколько, компонент Active Directory, называемый *глобальным каталогом*, позволяет клиентам одного домена получать информацию об объектах, расположенных в других доменах леса. В глобальном каталоге может быть лишь часть информации об объекте, но этого достаточно, чтобы найти более подробные сведения.

Ресурсы предприятия представлены в Active Directory в виде объектов или записей в БД. Каждый объект характеризуется рядом атрибутов или свойств. Например, у пользователя есть атрибуты имя пользователя и пароль, у группы — имя группы и список пользователей, которые в нее входят. Создав контроллер домена,

администратор заполняет его объектами. Служба Active Directory способна хранить миллионы объектов, включая пользователей, группы, компьютеры, принтеры, общие папки, сайты, связи сайтов, объекты групповой политики (ОГП) и даже зоны DNS и записи узлов.

Для объединения компьютеров и пользователей используются организационные подразделения (ОП). Групповая политика позволяет централизованно управлять практически любыми конфигурационными изменениями системы. С ее помощью можно настраивать параметры защиты, разворачивать программы и конфигурировать ОС и приложения, даже не прикасаясь к компьютерам пользователей. Вместо этого необходимые параметры настраиваются в объекте групповой политики и привязывают его к объекту-контейнеру Active Directory, содержащему объекты компьютеров и пользователей, которые нужно настроить.

Главным средством разрешения имен является DNS, но NetBIOS-имя домена по-прежнему имеет важное значение, особенно для клиентов, которые используют для именования службу NetBIOS.

В каждом домене имеется объект crossRef, используемый Active Directory для перенаправления запросов. Перенаправление запроса клиента происходит в том случае, когда в домене сервера каталога отсутствует объект, указанный в этом запросе. NetBIOS-имя домена хранится в объекте crossRef контейнера Partitions раздела конфигурации. Каждый объект crossRef имеет атрибут dnsRoot, в котором содержится полное DNS-имя домена, и атрибут netBIOSName, где указано его NetBIOS-имя.

Можно определить NetBIOS-имя домена с помощью графического пользовательского интерфейса. Для этого откройте оснастку Active Directory Domains and Trusts (Active Directory - домены и доверие) из группы *Администрирование*. На левой панели отметьте интересующий вас домен, щелкните на нем правой кнопкой мыши и выберите в открывшемся меню команду Свойства. В поле Domain name (pre-Windows 2000) (Имя домена (для версий операционных систем до Windows 2000)) будет указано NetBIOS-имя домена.

Также можно определить NetBIOS-имя домена с помощью интерфейса командной строки:

```
C:\Documents and Settings\Администратор>dsquery * cn=partitions,cn=configuration,dc=contoso,dc=com -filter "<(&(objectcategory=crossref)<(dnsroot=contoso.com)<(netbiosname=*))" -attr netbiosname
```

И, наконец, можно определить NetBIOS-имя домена с помощью сценария VBScript:

```
' ..... SCRIPT CONFIGURATION .....
```

```

strDomain = "povtas.ru" '
'.....END CONFIGURATION.....
set objRootDSE = GetObject("LDAP:///" & strDomain & "/RootDSE")
strADsPath = "<LDAP:///" & strDomain & "/cn=Partitions," & _
objRootDSE.Get("configurationNamingContext") & ">";
strFilter = "(&(objectcategory=Crossref)" & _
"(dnsRoot=" & strDomain & ")(netBIOSName=*))";
strAttrs = "netbiosname;"
strScope = "Onelevel"
set objConn = CreateObject("ADODB.Connection")
objConn.Provider = "ADsDSOObject"
objConn.Open "Active Directory Provider"
set objRS = objConn.Execute(strADsPath & strFilter & strAttrs &
strScope)
objRS.MoveFirst
WScript.Echo "NetBIOS name for " & strDomain & " is " &
objRS.Fields(0).Value

```

Консоли MMC

В повседневной работе администратор систем под управлением Windows Server 2003 часто использует служебные программы для конфигурирования учетных записей пользователей, модификации ПО и параметров служб, установки нового оборудования и т. д. Консоль MMC (Microsoft Management Console) - главный административный инструмент Windows Server 2003. Она консолидирует и организует наиболее часто используемые утилиты. Консоли MMC можно настраивать и приспособлять под конкретные потребности, поэтому ряд задач можно делегировать другим администраторам.

Консоль MMC предоставляет стандартный интерфейс для одного или нескольких прикладных модулей, называемых *оснастками* (snap-in), которые применяются для конфигурирования параметров среды. Эти оснастки приспособлены для решения конкретных задач, их можно упорядочивать и группировать в рамках консоли MMC. Почти все ярлыки в группе программ Администрирование это ссылки на готовые консоли MMC. Каждый из этих ярлыков открывает консоль MMC с единственной оснасткой (рис. 1.16.).

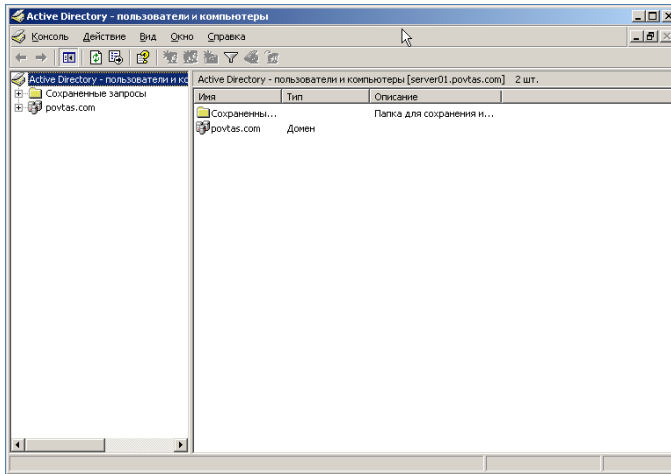


Рис. 1.16. Консоль Active Directory — пользователи и компьютеры

ММС поддерживает два типа оснасток: изолированные оснастки и оснастки-расширения. Изолированная оснастка, обычно называемая просто оснасткой, может быть добавлена к дереву консоли без предварительного добавления других элементов. Все средства администрирования для Windows Server 2003 являются либо консолями с одной оснасткой, либо преднастроенными сочетаниями оснасток, используемыми для решения конкретной категории задач. Оснастки-расширения, обычно называемые расширениями, всегда добавляются к другой изолированной оснастке или расширению, уже имеющимся в дереве консоли. Если для оснастки разрешены расширения, они работают с объектами, управляемыми оснасткой, такими как компьютер, принтер, модем или какое-нибудь другое устройство.

Когда оснастка или расширение добавляются к консоли, они могут появиться в виде нового элемента в дереве консоли или добавить новые пункты контекстного меню, дополнительные панели инструментов, дополнительные страницы свойств или мастера к оснастке, уже установленной в консоли.

Любую консоль можно настроить для работы в одном из двух режимов, авторском или пользовательском, причем в пользовательском режиме функциональность сохраненной консоли можно ограничить. При сохранении консолей в режиме по умолчанию (авторский режим) администратор получает доступ ко всей функциональности ММС. В этом случае администратор может

добавлять и удалять оснастки, создавать окна и задачи, просматривать узлы дерева консоли, сохранять и изменять параметры консоли. Если планируется распространять консоль, которая будет реализовывать конкретные функции, то можно задать необходимый пользовательский режим, а затем сохранить консоль. Пользовательские режимы, доступные при сохранении консоли ММС, приведены в таблице 1.1.

Таблица 1.1. Пользовательские режимы консоли ММС

Тип пользовательского режима	Описание
Полный доступ	Позволяет перемещаться по оснасткам, открывать окна и обращаться ко всем узлам дерева консоли.
Ограниченный доступ, несколько окон	Пользователи не вправе открывать новые окна или обращаться к узлам дерева, но могут просматривать в консоли несколько окон
Ограниченный доступ, одно окно	Пользователи не вправе открывать новые окна или обращаться к узлам дерева и могут просматривать в консоли только одно окно

Одна из самых мощных возможностей ММС - создание нестандартных консолей с любыми необходимыми оснастками. Для того чтобы создать свою оснастку с консолью *Просмотр событий* щелкните Пуск\Выполнить. Введите mms, затем щелкните ОК. Откроется окно *Консоль1 с Деревом консоли*. В меню Файл [Консоль] выберите Параметры, чтобы узнать, какой режим настроен для консоли. В раскрывающемся списке Режим консоли должен быть выбран Авторский режим. В меню Файл [Консоль] щелкните Добавить или удалить оснастку. Откроется диалоговое окно Добавить или удалить оснастку с выбранной вкладкой Изолированная оснастка. В окне Добавить или удалить оснастку щелкните Добавить, чтобы раскрыть окно Добавить изолированную оснастку. Выберите оснастку Просмотр событий, затем щелкните Добавить. Откроется диалоговое окно Выбор компьютера, в котором можно указать, какой компьютер вы хотите администрировать (локальный или удаленный). В итоге в дереве консоли появится новый узел — Просмотр событий (локальных). Сохраните консоль ММС.

Большинство оснасток позволяют управлять компьютерами пользователей через сеть. Эта возможность ММС одна из самых полезных, т.к. позволяет администратору управлять со своего

компьютера другими системами сети. Чтобы подключиться к другой системе с целями управления с помощью ММС, необходимо запустить из-под учетной записи с правами администратора на удаленном компьютере.

Службы терминалов

Службы терминалов устанавливаются по умолчанию вместе с ОС. На основе компьютера с Windows Server 2003 можно создать сервер служб терминалов. Службы терминалов позволяют совместно использовать приложения с помощью таких инструментов, как Дистанционное управление рабочим столом, Удаленный помощник и Сервер терминалов. Компьютер может параллельно обрабатывать до двух одновременных подключений удаленного рабочего стола без приобретения дополнительных лицензий. Добавив компонент *Сервер терминалов* и настроив соответствующую лицензию множество пользователей смогут запускать приложения на сервере.

В Windows Server 2003 встроены и установлены все компоненты, необходимые для поддержки удаленного рабочего стола. Для активации серверной части приложения необходимо на вкладке Удаленное использование окна *Система* выбрать переключатель Разрешить удаленный доступ к этому компьютеру, как показано на рисунке 1.17.

Подключение к удаленному рабочему столу — это клиентское приложение, используемое для подключения к серверу в контексте режима Дистанционное управление рабочим столом или Сервер терминалов. На компьютерах с Windows XP и Windows Server 2003 программа Подключение к удаленному рабочему столу установлена по умолчанию: Пуск\Все программы\Стандартные\Связь\Подключение к удаленному рабочему столу.

Можно управлять множеством параметров дистанционного подключения, как со стороны клиента, так и со стороны сервера. В табл. 1.3. перечислены конфигурационные параметры и их назначение.

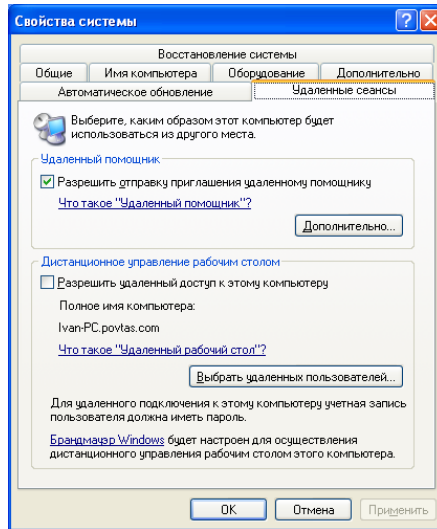


Рисунок 1.17. Вкладка Удаленное использование окна Система

Таблица 1.2. Параметры программы Удаленное подключение к рабочему столу

Параметры	Назначение
Общие	Позволяет выбрать компьютер, к которому необходимо подключиться, ввести статические реквизиты для входа в систему, а также сохранить параметры для данного подключения.
Экран	Содержит параметры, определяющие размер окна клиента, глубину цвета, а также отображение панели подключений при работе в полноэкранном режиме.

Продолжение Табл. 1.2.

Локальные ресурсы	Позволяет настраивать передачу звуковых событий с сервера на локальный компьютер, помимо стандартных выходных сигналов мыши, клавиатуры и экрана. Также параметры на этой вкладке определяют, как удаленный компьютер интерпретирует комбинации клавиш Windows, и доступны ли в сеансе удаленного доступа такие устройства, как
-------------------	---

	локальные диски, принтеры и последовательные порты.
Программы	Позволяет задавать путь и папки расположения для любых программ, которые необходимо запустить после установки соединения.
Дополнительно	Содержит параметры для настройки скорости соединения клиента и сервера, запрета отображения некоторых деталей рабочего стола сервера для экономии пропускной способности канала и снижения времени отклика удаленного подключения.

На рис. 1.18. показан клиент программы *Дистанционное подключение к рабочему столу*, настроенный для подключения к Server01 в домене povtas.com.

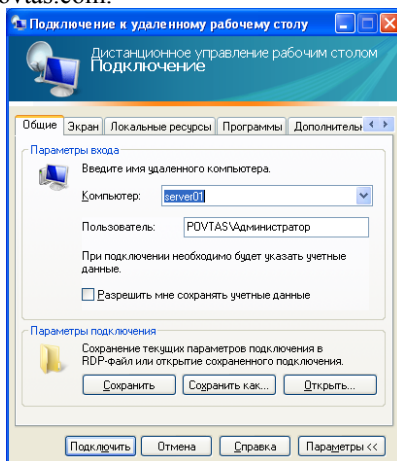


Рисунок 1.18. Подключение к удаленному рабочему столу

При использовании программы *Удаленный рабочий стол для администрирования* создается соединение между клиентом и сервером. Существует несколько потенциальных причин неудачных подключений или сбоев.

1. Ошибки в работе стандартной сети TCP/IP могут вызывать сбои или разрывы подключений службы терминалов. Если не функционирует служба DNS, клиент не сможет найти сервер по имени. Необходимо проверить настройки TCP/IP на стороне клиента и сервера, а также работу сетевого оборудования.

2. Неверно настроен порт Служб терминалов. По умолчанию это порт 3389 на клиенте и сервере. Если клиент и сервер настроены на использование различных портов, или этот порт заблокирован, подключение службы терминалов будет невозможным.

3. Для успешного подключения к серверу средствами программы Удаленный рабочий стол для администрирования пользователи должны быть включены в группу Администраторы или Пользователи удаленного рабочего стола. Сервер терминалов поддерживает только два удаленных подключения.

4. Только администраторам разрешено подключаться средствами программы Дистанционное подключение к рабочему столу к контроллерам доменов. Чтобы разрешить подключаться остальным пользователям, нужно настроить политику безопасности на контроллере домена.

5. Если сеансы прерывались без выхода из системы, сервер может посчитать, что достигнут предел одновременно обрабатываемых подключений, даже если в данный момент к серверу не подключены два пользователя. Например, клиент может завершить сеанс без выхода из системы и сервер считает это соединение открытым. Если еще два клиента попытаются подключиться к серверу, это удастся только одному из них.

Windows Messenger

У пользователей часто возникают проблемы с настройкой и использованием компьютера, разрешить которые по телефону достаточно сложно даже специалисту службы поддержки. Удаленный помощник предоставляет пользователям возможность получить помощь, облегчает и удешевляет работу корпоративных служб поддержки. Он позволяет пользователям запрашивать помощь у других клиентов сети, а те могут оказывать ее, наблюдая за тем, что происходит на экране компьютера, запросившего помощь. Кроме того, помощник может непосредственно руководить действиями запрашивающего помощь и демонстрировать ему правильные приемы, не посещая его компьютер лично. Удаленный помощник, или эксперт, может предложить помощь в разрешении проблем с компьютером.

Для работы программы *Удаленный помощник* необходимо, чтобы на обоих компьютерах была установлена ОС Windows XP или семейства Windows Server 2003.

Чтобы получить удаленную помощь, необходимо разрешить ее одним из следующих способов.

1. Через панель управления. С панели управления необходимо вызвать окно свойств системы и перейти на вкладку Remote. Поставьте флажок *Разрешить отправку приглашения удаленному помощнику*. Щелкнув на кнопку *Дополнительно*, можно указать, разрешено ли эксперту брать на себя управление удаленным компьютером, либо только наблюдать за действиями пользователя, а так же задать срок действия приглашений удаленной помощи.

2. Через групповую политику. При помощи консоли *Редактор объектов групповой политики*, gpedit.msc, откройте GPO домена или подразделения, содержащего компьютер клиента. Откройте контейнер Конфигурация компьютера\Административные шаблоны\Система\Удаленный помощник и включите политику *Запрошенная удаленная помощь*. Эта политика также позволит определить степень контроля эксперта над клиентским компьютером, срок действия приглашения и метод его пересылки по электронной почте. Политика *Предложение удаленной помощи* позволяет задавать имена пользователей и групп, которым разрешено быть экспертами, а также экспертов, которым разрешено управление либо только наблюдение за пользовательскими компьютерами.

Для получения удаленной помощи клиент должен создать приглашение и послать его эксперту одним из следующих способов:

1. Как сообщение Windows Messenger. Для отправки приглашений через службу Windows Messenger имя эксперта должно быть в списке контактов Windows Messenger. Личный запрос удаленной помощи возможен, только когда эксперт подключен к сети.

2. По электронной почте. Для отправки приглашения по электронной почте оба компьютера должны использовать MAPI-совместимый почтовый клиент.

3. Как файл. Разрешается также сохранить приглашение в файл и передать его эксперту любым методом, как вложение в почтовом сообщении, по FTP или на дискете.

Чтобы создать приглашение, выберите пункт *Справка и поддержка* в меню Start - откроется *Центр справки и поддержки*. Перейдите по *Приглашение для подключения Удаленного помощника* - откроется страница, показанная на рис. 1.19.

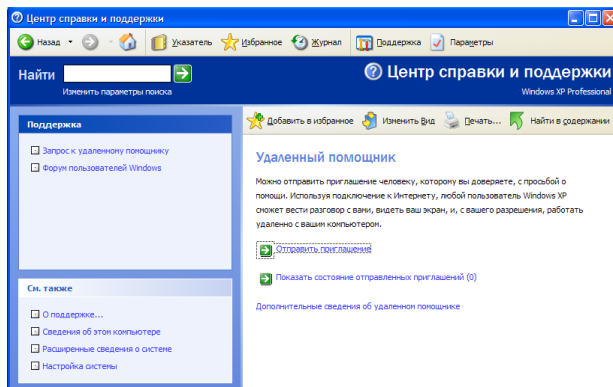


Рис. 1.19. Страница создания приглашения удаленного помощника

Перейдите по гиперссылке *Отправить приглашение* - откроется страница, показанная на рис. 1.20.

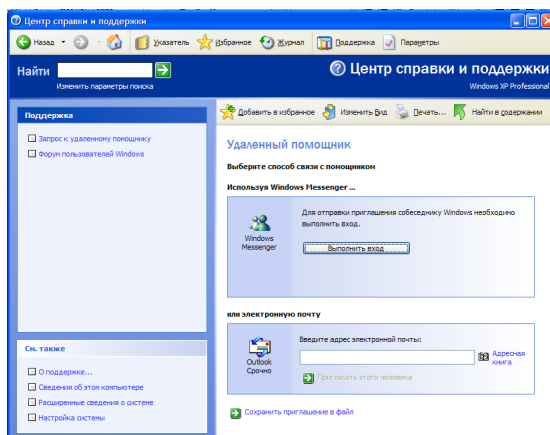


Рисунок 1.20. - Страница выбора способа связи с помощников

После установки удаленного подключения начинается сеанс *Удаленного помощника* на компьютере эксперта. Эксперт и пользователь могут совместно управлять рабочим столом, передавать файлы и использовать окно беседы, в котором они обсуждают возникшую проблему. Если для получения помощи пользователь решит отправить сообщение по электронной почте или запрос в виде файла, для установки сеанса удаленного помощника потребуется ввести общий пароль. Пользователь должен задать строгий пароль и

сообщить его эксперту по отдельному каналу связи (по телефону или в защищенном электронном письме).

При использовании программы *Удаленный помощник* следует учесть несколько моментов: можно сформировать открытую среду, в которой пользователи смогут получать удаленную помощь из-за пределов корпоративного брандмауэра, либо ограничить действие программы средствами групповой политики и указать различные уровни разрешений. Для внешних подключений необходимо открыть порт 3389.

Используя *Удаленный помощник*, неуполномоченный пользователь может учинить разрушения на удаленном компьютере. Чтобы свести этот риск к минимуму у *Удаленного помощника* существуют следующие защитные функции.

1. Защита приглашений. Никто не сможет подключиться к другому компьютеру через *Удаленного помощника* без приглашения. Клиенты должны устанавливать срок действия приглашений в минутах, часах или днях. Это не позволит эксперту подключиться к компьютеру пользователя после истечения срока действия приглашения.

2. Интерактивное подключение. Чтобы попытка эксперта подключиться к клиентскому компьютеру была успешной, пользователь должен быть на месте и предоставить эксперту доступ. *Удаленный помощник* нельзя использовать для подключения к компьютеру, оставленному без присмотра.

3. Контроль со стороны клиента. Последнее слово в управлении *Удаленным помощником* всегда принадлежит клиенту. Клиент может в любое время прервать подключение, нажав ESC.

4. Настройка удаленного управления. При помощи окна свойств системы и групповых политик *Удаленного помощника* пользователь и администратор определяют возможность и степень удаленного управления клиентским компьютером. Эксперт, имеющий доступ только для наблюдения, не сможет изменить конфигурацию пользовательского компьютера.

5. Брандмауэры. *Удаленный помощник* использует TCP-порт 3389. В сетях, подключенных к интернету, в которых также используется *Удаленный помощник*, рекомендуется закрывать этот порт на брандмауэрах, чтобы предотвратить передачу управления компьютером пользователям, расположенным за пределами сети.

2. Создание сценариев с помощью Microsoft Windows Script Host

Microsoft Windows Script Host (WSH) — компонент [Microsoft Windows](#), предназначенный для запуска сценариев на [скриптовых языках JScript](#) и [VBScript](#). Другими поставщиками программного обеспечения могут быть созданы обработчики сценариев (в виде ActiveX-объектов) для других языков, таких как Perl, TCL, REXX, и Python. В простейшем случае сценарий представляет собой это набор команд, записанный в тестовом файле [3, 4, 7].

Возможности сценариев на WSH далеко превосходят возможности командных .bat и .cmd-файлов: имеются полноценные языки с объектными возможностями, полный набор операций со строками, включая [регулярные выражения](#), взаимодействие с любыми программами, реализующими объектный скриптовый интерфейс, доступ к методам и [свойствам](#) их объектов; операции с [файлами](#) и каталогами, обработка текстовых файлов, манипуляции с [системным реестром](#) и т. п.

Существует две версии сервера сценариев Windows:

1. wscript.exe - позволяет задавать параметры выполнения сценариев в окне свойств.
2. cscript.exe - позволяет задавать параметры выполнения сценариев с помощью ключей командной строки.

Чтобы запустить необходимую версию, нужно ввести в командной строке wscript.exe или cscript.exe. Сервер Сценариев Windows встроен в Windows 98, Windows Me, Windows 2000, Windows XP и в Internet Information Services (начиная с версии 4.0).

Ранее единственным встроенным языком сценариев, поддерживаемым Windows, был язык команд MS-DOS. Хотя этот язык является достаточно быстрым и компактным, он имеет ограниченные возможности по сравнению с языками Visual Basic Script и JavaScript. На сегодняшний день Сервер Сценариев Windows позволяет пользователям использовать преимущества мощных языков сценариев, таких как Visual Basic Script и JavaScript. Язык команд MS-DOS также поддерживается.

Способы выполнения сценариев Windows

Архитектура ActiveX, реализующая выполнение сценариев, позволяет использовать такие языки как VBScript, JavaScript, и Perl. В настоящее время Microsoft предоставляет возможность выполнять

сценарии на этих языках при помощи трех видов серверов (контроллеров) на платформе Windows:

1. Microsoft Internet Explorer. Позволяет выполнять сценарии, содержащиеся в HTML-страницах, на клиентских машинах.

2. Internet Information Services (IIS). Поддерживает технологию ASP (Active Server Pages), позволяющую запускать сценарии, на Web-серверах. Это используется для автоматической генерации передаваемых клиенту через Internet или по внутренней сети страниц.

3. Сервер Сценариев Windows (WSH). Позволяет выполнять сценарии непосредственно в графическом окне Windows или в текстовой консоли, при этом нет необходимости встраивать тексты сценариев в документ HTML. Сценарии могут быть запущены напрямую щелчком мыши на файле сценария в Проводнике Windows либо из командной строки консоли. WSH не требует много оперативной памяти и удобен для выполнения задач, не требующих взаимодействия с пользователем, таких как написание сценариев входа (logon), для выполнения административных задач. При запуске сценария с рабочего стола или из командной строки сервер сценария читает и передает содержимое указанного файла зарегистрированному обработчику сценариев. Для определения языка сценария используется расширение имени файла (.vbs для VBScript и .js для JScript).

Для использования WSH на компьютере должен быть установлен Microsoft Internet Explorer версии не ниже 3.0. Сервер сценариев использует обработчики сценариев для языков Visual Basic Script и JavaScript, встроенные в Internet Explorer.

Для выполнения сценариев с помощью сервера сценариев для командной строки (cscript.exe) предусмотрен следующий синтаксис:

**cscript [имя_сценария] [параметры_сервера]
[аргументы_сценария]**

- имя_сценария — имя файла сценария, включая путь и расширение;
- параметры_сервера — ключи командной строки, задающие различные свойства сервера сценариев Windows. Параметр сервера всегда начинается с двух косых черт (/);
- аргументы_сценария — ключи командной строки, которые передаются в сценарий. Аргумент сценария всегда начинается с одной косой черты (/).

Вышеперечисленные параметры являются необязательными. Но нельзя задать аргументы сценария, не задав сценарий. При отсутствии аргументов сценария или самого сценария программа cscript.exe

выведет описание синтаксиса команды и предусмотренные ключи, которые перечислены в таблице 2.1.

Таблица 2.1 Ключи сервера сценариев для командной строки

Ключ	Назначение
//B	Включение пакетного режима. Подавляется отображение ошибок и запросов сценария
//D	Включение режима Active Debugging (отладчика)
//E:ядро	Использование указанного ядра для выполнения сценария
//H:cscript	Стандартный сервер сценариев заменяется на CScript.exe
//H:wscript	Стандартный сервер сценариев заменяется на WScript.exe (по умолчанию)
//I	Включение диалогового режима, в котором выводятся подсказки и сообщения об ошибках. Применяется по умолчанию, отменяет ключ //B.
//Job:xxxx	Выполнение задания xxxx, указанного в файле сценария .wsf
//Logo	Отображать сведения о программе. Применяется по умолчанию, отменяет режим //Nologo
//Nologo	Не отображать сведения о программе во время выполнения
//S	Сохранение текущих параметров командной строки для данного пользователя
//T:nn	Указание максимального времени (в секундах), отведенного на выполнение сценария. Можно указать значение времени до 32 767 секунд. По умолчанию время выполнения не ограничено. Если время выполнения превышает заданную величину, cscript.exe прерывает работу обработчика и останавливает процесс.
//X	Выполнение сценария в отладчике

//U	Использование кодировки Юникод при перенаправлении ввода-вывода с консоли
-----	---

Для использования сервера сценариев Windows можно создать файл .wsf, позволяющий вызывать несколько обработчиков сценариев и выполнить несколько заданий, в том числе, написанных на разных языках сценариев.

Существует несколько способов запуска сценария в окне Windows:

1. Двойным щелчком мышью по ярлыку или файлу в окне "Мой компьютер", "Поиск" или в окне Проводника Windows;
2. С использованием команды Windows "Выполнить..." - вызвать wscript.exe с именем и параметрами сценария (либо сделать то же самое из командной строки Windows).

Если расширение файла сценария еще не связано с программой wscript.exe, то появится диалоговое окно "Открыть с помощью", в котором нужно выбрать программу, с помощью которой нужно открывать этот файл сценария. Программа wscript будет зарегистрирована как приложение по умолчанию для запуска всех файлов с данным расширением, если после выбора программы "Сервер сценариев Windows" (wscript.exe) установить флажок "Использовать ее для всех файлов такого типа". Например, если установить этот флажок при запуске программы с расширением .vbs, то wscript.exe станет приложением по умолчанию для запуска всех программ с таким расширением.

В Windows Server 2003 можно настраивать сценарии четырех типов, которые выполняются:

1. во время загрузки компьютера;
2. перед завершением работы компьютера;
3. при входе пользователя в систему;
4. при выходе пользователя из системы.

Эти сценарии могут быть командными файлами с расширением .bat или .cmd или сценариями для WSH.

Сценарии загрузки компьютера и завершения работы назначаются как часть групповой политики. Таким образом, все компьютеры — члены сайта, домена и/или ОП — автоматически исполняют сценарии при загрузке или завершении работы. Сценарии загрузки компьютера можно указать в виде назначенных заданий с помощью Мастера планирования заданий (Scheduled Task Wizard).

Практически каждая операция в Active Directory выполняется с использованием различных средств. При этом почти все задачи выполняются как минимум тремя способами:

1. с помощью одной из утилит с графическим пользовательским интерфейсом (например, оснастки MMC);
2. с использованием одной из утилит с интерфейсом типа командной строки (например: dsadd, dsmod, dsrm, dsquery, dsget, nltest, netdom или ldifde);
3. программным путем — с помощью сценария, написанного на VBScript или Perl.

Выбор метода зависит от предпочтений администратора и от ситуации, в которой возникла проблема. Одним из недостатков языка VBScript является то, что он не предназначен для выполнения сложных задач (в тех случаях, когда решить проблему с его помощью трудно, часто используют язык Perl).

Протокол LDAP

Служба каталогов Active Directory основана на протоколе LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам) [3, 7]. Это протокол прикладного уровня для доступа к службе каталогов X.500, разработанный как облегченный вариант протокола DAP. LDAP — относительно простой протокол, использующий TCP/IP и позволяющий производить операции аутентификации (bind/unbind), поиска (search), сравнения (compare) и операции модификации (add, delete, modrdn, modify). Обычно LDAP-сервер принимает входящие соединения на порт 389 по протоколам TCP или UDP. Для LDAP-сеансов, инкапсулированных в SSL, используется порт 636.

Любая запись в каталоге LDAP обладает уникальным именем (DN — Distinguished Name) и состоит из одного или нескольких атрибутов. Уникальное имя может выглядеть следующим образом: «cn=Иван Петров, ou=Сотрудники, dc=povtas, dc=com». Уникальное имя состоит из одного или нескольких относительных уникальных имен (RDN — Relative Distinguished Name), разделенных запятой. Относительное уникальное имя имеет вид ИмяАтрибута=значение. На одном уровне каталога не может существовать двух записей с одинаковыми относительными уникальными именами. В силу такой структуры уникального имени записи в каталоге LDAP можно легко представить в виде дерева.

Запись может состоять только из тех атрибутов, которые определены в описании класса записи (object class), которые, в свою очередь, объединены в схемы (schema). В схеме определено, какие атрибуты являются для данного класса обязательными, а какие —

необязательными. Также схема определяет тип и правила сравнения атрибутов. Каждый атрибут записи может хранить несколько значений.

Определение переменных и обработка ошибок

Важной частью любого сценария являются инструкции, предназначенные для обработки ошибок. Такие инструкции позволяют своевременно выявить возникшую при выполнении той или иной части сценария ошибку и предпринять соответствующие действия, не прекращая его работы. В рассматриваемых примерах большинство сценариев не содержит кода обработки ошибок, предопределенных переменных или, например, кода, освобождающего занимаемую переменными память. Такие сценарии должны быть короткими и не могут содержать дополнительный код, который бы их сильно загромождал. Поэтому их нельзя считать надежными и устойчивыми программами, способными корректно работать при любых обстоятельствах. Это скорее заготовки, которые позволяют быстро выполнить типичную задачу в стандартном окружении и на основе которых при желании можно написать собственный, более гибкий и надежный, код.

VBScript является регистронезависимым языком (в отличие от JavaScript). Изменение регистра символов (с прописных на строчные и наоборот) в имени переменной приводит к одной и той же переменной. Например, `variable`, `Variable` и `vaRiabLe` — одинаковые переменные.

Обработка ошибок в VBScript выполняется следующим образом. Текст сценария начинается со строки `On Error Resume Next`.

Она указывает интерпретатору, что в случае возникновения ошибки, выполнение сценария нужно продолжать. Если сценарий не содержит такой инструкции, его выполнение прекращается при первой же ошибке. При наличии инструкции `On Error Resume Next` далее в сценарии должен располагаться программный код, в котором осуществляется проверка объекта `Err` на наличие ошибок. Такой код должен следовать за любым фрагментом сценария, где выполняются действия, способные привести к ошибкам. Вот простейший пример:

```
On Error Resume Next
Set objDomain =
GetObject("LDAP://dc=povtas.dc=com")
If Err.Number<>0 then
    Wscript.Echo "При попытке получить объект
домена произошла ошибка: "& Err.Description
Wscript.Quit
```

End if

Двумя важнейшими свойствами объекта Err являются Number, ненулевое значение которого указывает на наличие ошибки, и Description, содержащее текстовое сообщение об ошибке.

Желательно в начало каждого сценария помещать следующую строку: Option Explicit.

Установление этой команды означает, что каждая используемая в сценарии переменная должна быть объявлена, в противном случае при выполнении сценария будет сгенерировано исключение.

Переменные в VBScript объявляются с помощью ключевого слова Dim. Завершив работу с переменной, следует присвоить ей значение Nothing, чтобы вернуть системе связанные с ней ресурсы. Кроме того, эта мера помогает предотвратить случайное повторное использование переменной со старым значением. В следующем примере продемонстрировано, как дополнить приведенный выше сценарий, выводящий имя домена, кодом обработки ошибок и управления переменными:

```
Option Explicit
On Error Resume Next
Dim objDomain
set objDomain =
GetObject ("LDAP://cn=users.dc=povtas.dc=com")
if Err.Number<>0 then
    Wscript.Echo "При попытке получить объект
домена произошла ошибка: " & Err.Description
    Wscript.Quit
end if

Dim strDescr
strDescr = objDomain.Get("description")
if Err.Number<>0 then
    Wscript.Echo "При попытке получить описание
домена произошла ошибка: " & Err.Description
    Wscript.Quit
end if
WScript.Echo "Description: " & strDescr
objDomain = Nothing
strDescr = Nothing
```


3. Учетные записи пользователей

Учетная запись пользователя - это набор данных, сообщающих операционной системе к каким папкам и файлам пользователь имеет доступ, какие он может делать изменения в работе компьютера, а также персональные настройки пользователя, такие как настройки и цветовое оформление рабочего стола. Учетные записи пользователей позволяют осуществлять работу нескольких пользователей на компьютере, каждый из которых будет иметь свои собственные файлы и настройки. Каждый пользователь получает доступ к своей учетной записи с помощью имени пользователя и пароля. Учётная запись содержит сведения, необходимые для идентификации пользователя при подключении к системе, а также информацию для [авторизации](#) и [учёта](#).

В Active Directory перед разрешением доступа к ресурсам проводится проверка подлинности пользователя на основе его учетной записи, которая содержит имя для входа в систему, пароль и уникальный *идентификатор безопасности* (security identifier, SID). В процессе входа в систему Active Directory проверяет подлинность имени и пароля. После этого подсистема безопасности может создать маркер доступа, представляющий этого пользователя. В маркере доступа содержатся SID учетной записи пользователя и SID всех групп, к которым относится пользователь. При помощи этого маркера можно проверить назначенные пользователю права, в том числе право локально входить в систему, а также разрешить или запретить доступ к ресурсам, защищенным *таблицами управления доступом* (access control list, ACL) [1, 5, 9].

Учетная запись пользователя интегрирована в объект пользователя в Active Directory. В объекте пользователя хранятся не только имя, пароль и SID, но также контактная информация (например, номера телефонов и адреса), организационная информация, в том числе должность, прямые подчиненные и руководитель, сведения о членстве в группах и конфигурации, например параметры перемещаемого профиля, служб терминалов, удаленного доступа и удаленного управления. Каждый пользователь должен иметь учетную запись.

Существуют три типа учетных записей:

1. Стандартная. Стандартная учетная запись позволяет использовать большую часть возможностей компьютера, но если необходимо сделать изменения, влияющие на всех пользователей или на безопасность компьютера, то потребуется разрешение

администратора. Используя стандартную учетную запись, можно работать в большинстве установленных на компьютере программ, но устанавливать новые или удалять старые программы и устройства, удалять необходимые для работы компьютера файлы и изменять настройки, влияющие на всех пользователей компьютера, нельзя. Если используется стандартная учетная запись, некоторые программы могут потребовать пароль администратора для выполнения каких-либо задач.

2.Администратор. Учетная запись администратора представляет собой учетную запись пользователя, с помощью которой можно делать изменения, затрагивающие других пользователей компьютера. Администраторы имеют доступ ко всем функциям ОС, могут менять параметры безопасности, устанавливать программное обеспечение и оборудование. Кроме того, администраторы могут изменять любые учетные записи пользователей. При установке Windows потребуется создать учетную запись администратора, позволяющей настраивать компьютер и устанавливать любые программы. После окончания настройки компьютера для повседневного использования рекомендуется использовать стандартную учетную запись. Безопаснее использовать стандартную учетную запись пользователя вместо учетной записи администратора.

3.Гость. Эта учетная запись предназначена для временных пользователей, не имеющих постоянной учетной записи на компьютере или в домене. Она позволяет использовать компьютер без доступа к личным файлам. Пользователи, вошедшие в систему под учетной записью «Гость», не могут устанавливать программное обеспечение и оборудование, изменять настройки или создавать пароль. Эта запись создается во время установки ОС и остается в отключенном состоянии и не имеет пароля, поэтому нужно включить учетную запись гостя, прежде чем кто-либо сможет ее использовать для входа в систему. Рекомендуется оставлять ее заблокированной, а для пользователей, нуждающихся в доступе к системе, создавать индивидуальные учетные записи.

Планирование учетных записей пользователей

Прежде чем создавать учетные записи для пользователей, следует сформулировать свои правила назначения имен, паролей с учетом иерархии Active Directory. Это особенно важно в случае большой и сложной сети.

При создании локальной или доменной учетной записи пользователя администратор указывает реальные фамилию и имя пользователя, но для входа и проверки подлинности будет

применяться имя учетной записи. Имя учетной записи должно быть уникально. Длина имени не должна превышать 64 символов. Имена не чувствительны к регистру, в них запрещается использовать следующие символы:

“ / \ [] : ; | = , + * ? < > @.

Следует учитывать, что имена учетных записей также используются в адресах электронной почты. Поэтому необходимо следить за соблюдением всех ограничений, которые почтовое ПО налагает на имена пользователей.

В организациях часто образуют имена учетных записей из инициалов и фамилии, либо имени пользователя. Например, имя учетной записи пользователя Иван Иванов может быть ИИванов или ИванИ. Когда пользователей много, этот способ становится неудобным, поскольку вероятно существование пользователей с одинаковыми именами и фамилиями, начинающимися на одинаковые буквы. Необходимо разработать соответствующие правила для назначения имен пользователей и строго их придерживаться.

Назначение несогласованных имен учетных записей ведет к путанице и затрудняет другим администраторам поиск пользователей по именам учетных записей. Необходимы правила, предусматривающие стандартные комбинации инициалов, имен и фамилий, а также действия на тот случай, когда правила дают идентичные имена. Эти правила должны позволить администратору с достаточной уверенностью «вычислить» по имени незнакомого пользователя имя его учетной записи. Также можно для временных пользователей указывать префикс В- (например, В-П_Петров).

При создании учетной записи следует задать ей пароль, а также выбрать политику управления паролями учетных записей, которая определяется степенью безопасности, требуемой в организации. Active Directory в Windows Server 2003 поддерживает политики безопасности, обеспечивающие сложность паролей и их безопасное использование в рамках предприятия. Рядовой сервер под управлением Windows Server 2003 поддерживает политику для своих локальных учетных записей пользователей, которая настраивается из оснастки *Локальная политика безопасности*.

Политика учетных записей домена управляется посредством ОГП Default Domain Policy. Изменять заданные по умолчанию правила назначения паролей можно редактируя при помощи оснастки Group Policy Object Editor (Редактор объектов групповой политики) параметры политики паролей. Наиболее часто настраивают политику в отношении объектов пользователей домена. Политики паролей домена

позволяют защищать сеть путем внедрения лучших методик управления паролями, проверенных практикой. Эти политики описаны в таблице 3-1.

Таблица 3.1. Параметры политики паролей

Политика	Описание
Требовать неповторяемости	Включена по умолчанию, максимальное значение - 24. Active Directory хранит список недавно использованных паролей и не разрешает пользователю задавать пароль из этого списка.
Максимальный срок действия пароля	Значение по умолчанию - 42 дня. Определяет, как долго может использоваться пароль, прежде чем Active Directory заставит пользователя сменить его.
Минимальный срок действия пароля	Значение по умолчанию — 1 день. Определяет, как долго может использоваться пароль, прежде чем Active Directory разрешит пользователю сменить его. Пользователю запрещено менять пароль более одного раза в течение указанного в этом параметре периода времени.
Минимальная длина пароля	Значение по умолчанию — 7 символов. Определяет минимальное число символов, которое Active Directory разрешает вводить пользователям при смене пароля.
Пароль должен отвечать требованиям сложности	В Windows Server 2003 эта политика включена по умолчанию. Задаёт критерии сложности пароля, такие как длина (не менее шести символов), запрет дублирования имени учетной записи в качестве пароля, требование наличия в пароле не менее трех символов из следующих категорий: буквы в нижнем и верхнем регистре, цифры и не алфавитно-цифровые символы.

Для новых объектов пользователей по умолчанию также активируется параметр Потребовать смену пароля при следующем входе в систему. Предполагается, что пользователь самостоятельно введет известный только ему пароль и будет регулярно менять его. Таким образом, администратору достаточно указать временный пароль для первого входа пользователя в систему.

Создание объектов пользователей

Создать объект пользователя проще всего в консоли Active Directory — пользователи и компьютеры. Рекомендуется создавать объект пользователя в организационном подразделении (ОП), чтобы в полной мере задействовать делегирование административных полномочий и объекты групповой политики (ОГП).

Чтобы создать объект пользователя, необходимо выбрать нужный контейнер, затем в меню *Действие* щелкнуть *Создать Пользователь*. Для этого нужно быть членом групп Администраторы предприятия, Администраторы домена или Операторы учета, либо вам должны быть делегированы административные полномочия. В противном случае команда создания будет недоступна.

Откроется диалоговое окно *Новый объект — Пользователь*, (рис. 3.1.), в котором необходимо ввести сведения об имени пользователя.

Рис. 3.1. Диалоговое окно Новый объект — Пользователь

Свойства пользователя на первой странице окна *Новый объект — Пользователь* описаны ниже:

- **Имя.** Имя пользователя. Не обязательный параметр.
- **Инициалы.** Инициалы пользователя. Не обязательный параметр.
- **Фамилия.** Фамилия пользователя. Не обязательный параметр.
- **Полное имя.** Полное имя пользователя. Если указано имя или фамилия пользователя, значение этого поля будет заполнено

автоматически. Это обязательное поле. Можно изменить предложенное значение. На основе введенного здесь имени генерируется несколько свойств объекта пользователя, в частности CN (обычное имя), DN (различающееся имя), name (имя) и displayName (отображаемое имя). Т.к. значение CN должно быть в контейнере уникальным, введенное здесь имя должно быть уникальным среди остальных объектов в ОП (или другом контейнере), где создается объект пользователя.

- **Имя входа пользователя.** Имя участника-пользователя (user principal name, UPN) состоит из имени пользователя для входа и суффикса UPN, которым по умолчанию является DNS-имя домена, в котором создается объект. Это свойство обязательно, а UPN-имя в целом (в формате имя_входа@суффикс-UPN) должно быть уникальным в лесу Active Directory.

- **Имя входа пользователя (пред-Windows 2000).** Используется для входа в систему с клиентов под управлением более ранних версий Windows, например Windows 9x/Me/NT 4 или Windows NT 3.51. Это поле является обязательным и должно быть уникальным в домене. Заполняется автоматически символами (не более 20), взятыми из введенного ранее имени входа.

Закончив ввод значений, щелкните *Далее*. Затем необходимо ввести пароль пользователя и установить управляющие флажки учетной записи (рис. 3.2.).

Рис. 3.2. Вторая страница окна Новый объект — Пользователь

В таблице 3.2. перечислены свойства со второй страницы окна *Новый объект — Пользователь*.

Таблица 3.2. Свойства пользователя на второй странице окна *Новый объект — Пользователь*

Свойство	Описание
Пароль	Максимум - 127 символов. Пароль будет использоваться для проверки подлинности пользователя. В целях безопасности пароль необходимо задавать всегда.
Подтверждение	Повторный ввод пароля во избежание опечаток. Если пароли, введенные и в предыдущем и в этом полях, не совпадают, потребуются повторить ввод пароля.
Требовать смену пароля при следующем входе в систему	Следует установить этот флажок, если нужно, чтобы пользователь изменил пароль, введенный вами при первом входе в систему. Параметр недоступен, если установлен флажок <i>Срок действия пароля не ограничен</i> .
Запретить смену пароля пользователем	Следует установить этот флажок, если одной учетной записью в домене пользуются несколько человек или если необходимо контролировать пароли учетной записи этого пользователя. Обычно этот параметр используется для управления паролями учетных записей служб. Его нельзя выбрать, если установлен флажок <i>Требовать смену пароля при следующем входе в систему</i> .
Срок действия пароля не ограничен	Следует установить этот флажок, если хотите, чтобы срок действия пароля не истекал. При этом флажок <i>Требовать смену пароля при следующем входе в систему</i> будет автоматически снят, так как это взаимоисключающие параметры. Обычно используется для управления паролями учетных записей служб.
Отключить учетную запись	Этот флажок отключает учетную запись пользователя. Он удобен при создании объекта для только что нанятого сотрудника, которому пока не требуется входить в сеть.

При создании объектов новых пользователей для каждого из них следует назначать уникальные сложные пароли, не отвечающие какому-либо предсказуемому шаблону. Если пользователь не будет входить в сеть долгое время, необходимо отключить его учетную

запись. Когда пользователю в первый раз потребуется доступ к сети, убедитесь, что его учетная запись включена. Active Directory попросит пользователя задать новый уникальный пароль, известный только ему.

Некоторые из параметров учетных записей, перечисленных в таблице 3.3, могут противоречить политикам, настроенным в домене. Например, в политике домена по умолчанию хранение паролей с использованием обратимого шифрования выключено. Однако в редких случаях, требующих обратимого шифрования, значение свойства учетной записи *Хранить пароль, используя обратимое шифрование* для данного объекта пользователя будет иметь приоритет. Также в домене может быть указан максимальный срок действия пароля, или пользователь должен будет изменить пароль при следующем входе в систему. Если объект пользователя настроен так, что срок действия пароля не ограничен, эти настройки перекроют политики домена.

Управление учетными записями пользователей

При создании объекта пользователя требуется настроить общие свойства пользователя, в том числе имена для входа и пароль. Для управления свойствами созданных объектов пользователей используется консоль Active Directory — пользователи и компьютеры. Чтобы настроить свойства объекта пользователя, выберите объект и в контекстном меню или в меню Действие щелкните Свойства. Откроется окно Свойства для этого объекта (рис. 3.3.).

Рис. 3.3. Диалоговое окно *Свойства* для объекта пользователя

Особого внимания заслуживают свойства учетной записи пользователя на вкладке *Учетная запись* диалогового окна *Свойства*

пользователя (рис. 3.4.). Некоторые свойства настраиваются при создании объекта пользователя, и их, как и большой набор других свойств учетной записи.

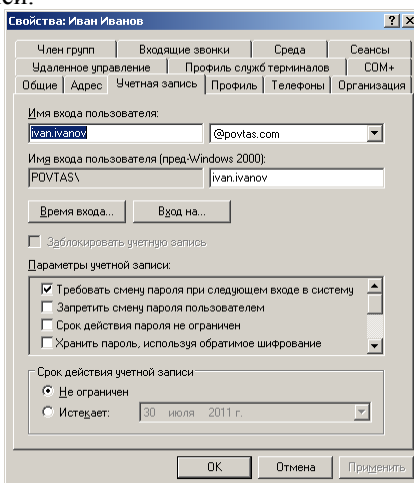


Рис. 3.4. Вкладка Учетная запись объекта пользователя

Значения некоторых свойств представлены ниже:

- **Время входа.** Отображается окно Время входа, в котором можно настроить время и дни недели, когда пользователю разрешено входить в сеть. Если разрешенное время входа истекло, в то время когда пользователь еще находится в системе, его сеанс не прерывается.

- **Вход на.** Используется для запрета пользователю входить в систему с некоторых рабочих станций. В других окнах эта функция называется Ограничения компьютера (Computer Restrictions). Для работы этой функции необходимо включить NetBIOS поверх TCP/IP, так как ограничение применяется к имени компьютера, а не к MAC-адресу его сетевой платы.

- **Заблокировать учетную запись.** Флаг по умолчанию снят. Он устанавливается, когда учетная запись пользователя блокируется из-за большого числа неудачных попыток входа в систему. Для разблокирования учетной записи необходимо снять этот флаг.

- **Хранить пароль, используя обратимое шифрование.** Этот параметр позволяет хранение пароля в Active Directory с использованием обратимого шифрования вместо более мощного алгоритма для необратимого шифрования. Он предназначен для поддержки приложений, которым требуется знать пароль

пользователя. Если в этом нет крайней необходимости, не следует включать этот параметр, так как он существенно ослабляет безопасность пароля. Пароли, которые хранятся с использованием обратимого шифрования, — это практически то же самое, что пароли, записанные открытым текстом.

- **Отключить учетную запись.** Включение и отключение учетной записи пользователя.

- **Для интерактивного входа в сеть нужна смарт-карта.** Смарт-карты — это переносные устройства, защищенные от несанкционированного вмешательства, на которых хранится уникальная идентификационная информация пользователя. Они присоединяются или вставляются в системное устройство и являются дополнительным физическим идентификационным компонентом процесса проверки подлинности.

- **Учетная запись доверена для делегирования.** Этот параметр позволяет учетной записи службы выдавать себя за пользователя, чтобы обращаться к сетевым ресурсам от его имени. Обычно этот параметр не включают, особенно для объектов, представляющих людей.

- **Учетная запись важна и не может быть делегирована.** Активация этого параметра запрещает делегирование учетной записи другими учетными записями.

- **Использовать DES-шифрование для этой учетной записи.** Этот параметр заставляет Active Directory использовать шифровальный алгоритм DES для объектов пользователей.

- **Без предварительной проверки подлинности Kerberos.** Этот параметр заставляет Active Directory опустить предварительную проверку подлинности по протоколу Kerberos при проверке подлинности пользователя. Это снижает защиту протокола, поэтому не стоит включать данный параметр без причин.

- **Срок действия учетной записи.** Задается дата окончания действия учетной записи, при наступлении которой учетная запись автоматически блокируется.

Windows Server 2003 позволяет одновременно изменять свойства нескольких учетных записей пользователей. Для этого нужно выбрать несколько объектов пользователей и в меню Действие щелкнуть Свойства. Можно выбирать только однотипные объекты.

Для нескольких объектов пользователей одновременно можно изменить следующие свойства:

1. Вкладка Общие: свойства Описание, Комната, Номер телефона, Факс, Веб-страница, Адрес электронной почты.

2. Вкладка Учетная запись: свойства Суффикс UPN, Время входа, Вход на, Параметры учетной записи, Срок действия учетной записи истекает.

3. Вкладка Адрес: свойства Улица, Почтовый ящик, Город, Штат/Область, Почтовый индекс, Страна/Регион.

4. Вкладка Профиль: свойства Путь к профилю, Сценарий входа и Домашняя папка.

5. Вкладка Organization: свойства Должность, Отдел, Организация, Руководитель.

Кроме вышеперечисленных, имеется множество свойств, которые для каждого пользователя должны настраиваться отдельно. Кроме того, определенные административные задачи, в том числе изменение паролей и переименование учетных записей, должны выполняться отдельно для каждого объекта пользователя.

Если пользователь переводится на другую должность, может понадобиться переместить его объект, чтобы отразить изменения в управлении или настройках объекта: выберите его в Active Directory — пользователи и компьютеры и в контекстном меню или в меню Действие щелкните Переместить. Также можно перемещать объекты между ОП, просто перетаскивая их в консоли Active Directory — пользователи и компьютеры.

Создание нескольких объектов пользователей

Очень часто объекты могут обладать одинаковыми свойствами. Например, все студенты одного курса могут принадлежать одной группе безопасности, им всем может быть разрешен вход в систему в одно и то же время, а их папки и перемещаемые профили могут храниться на одном сервере. В таких случаях при создании объекта пользователя целесообразно предварительно задать для него общие свойства. Для этого можно создать универсальный объект пользователя, часто называемый шаблоном, и для создания новых объектов пользователей копировать этот объект.

Чтобы создать шаблон объекта пользователя, создайте новый объект пользователя и настройте его свойства. Поместите пользователя в требуемые группы. Чтобы эта учетная запись не была использована для доступа к сетевым ресурсам, следует отключить данного пользователя, так как это всего лишь шаблон.

Для создания объекта пользователя на основе шаблона, укажите нужный шаблон и в меню Действие щелкните Копировать.

Потребуется задать некоторые свойства: имя и фамилию, инициалы, имя входа, пароль и параметры учетной записи. После создания объекта можно видеть, что свойства были скопированы из шаблона (таблица 3.3).

Таблица 3.3. Свойства, значения которых копируются из шаблона

Вкладка	Свойства
Общие	Свойства не копируются.
Адрес	Копируются все свойства, кроме Улица.
Учетная запись	Копируются все свойства, кроме имени входа.
Профиль	Копируются все свойства, пути к профилю и домашней папке изменяются в соответствии с именем для входа нового пользователя.
Телефоны	Свойства не копируются.
Организация	Копируются все свойства, кроме Должность.
Член групп	Копируются все свойства.
Входящие звонки	Свойства не копируются
Среда	Свойства не копируются
Сеансы	Свойства не копируются
Удаленное управление	Свойства не копируются
Профиль служб терминалов	Свойства не копируются
SOM+	Свойства не копируются

Пользователь, объект которого был создан из шаблона, входит в те же группы, что и шаблон, то есть получает разрешения и права, назначенные этим группам. Однако разрешения и права, явно назначенные самому шаблонному объекту пользователя, не копируются и не переназначаются.

Импорт объектов пользователей при помощи CSVDE

Инструмент CSV Directory Exchange (csvde.exe) — это утилита командной строки, позволяющая импортировать и экспортировать объекты в Active Directory из (в) текстового файла с разделителями—запятыми. Текстовый файл с разделителями-запятыми представляет собой обычный текстовый файл с содержимым базы данных. Каждая запись представлена отдельной строкой, а поля записей разделены запятыми. Формат широко распространен и читается такими программами, как *Блокнот* и Microsoft Excel.

Эта команда представляет собой мощный инструмент для быстрой генерации объектов. Ее базовый синтаксис таков:

csv -{-de [- i] [-f имя-файла] [-k]

где:

- i — переключает команду в режим импорта; если не указан, по умолчанию включается режим экспорта;

- f *имя-файла* — задает имя импортируемого файла;

-k — во время импорта игнорирует ошибки и продолжает процесс.

Импортируемый файл является текстовым файлом с разделителями—запятыми (*.csv или *.txt), где первая строка представляет собой список имен в формате протокола LDAP для импортируемых атрибутов, вслед за которой на отдельных строках перечисляются все объекты. Для каждого объекта должны быть указаны те атрибуты, которые перечислены в первой строке. Например, файл может быть таким:

```
DN,objectClass,SamAccountName,sn,givenName,userPrincipalName
"CN=Андрей Калиберда,OU=Employees, DC=povtas, DC=com",
user, andrey.kalib, Калиберда, Андрей, andrey.kalib@povtas.com
```

Если импортировать этот файл, то в ОП Employees будет создан объект пользователя с именем Андрей Калиберда. Имена для входа, имя и фамилия задаются согласно данным из файла. Первоначально этот объект будет отключен, включить его можно после смены пароля.

Использование средств командной строки Active Directory

Windows Server 2003 поддерживает множество мощных средств командной строки, упрощающих управление Active Directory:

- DSADD — добавляет объекты в каталог;
- DSGET — отображает («получает») свойства объектов каталога;
- DSMOD — изменяет выбранные атрибуты существующего объекта каталога;
- DSMOVE — перемещает объект из текущего контейнера в новое местоположение;
- DSRM — удаляет объект или все дерево ниже объекта по иерархии, либо удаляет и объект, и дерево;
- DSQUERY — запрашивает в Active Directory объекты, отвечающие указанным условиям поиска; эту команду часто используют для создания списка объектов, который затем передается по каналу другому средству командной строки для анализа или модификации.

В параметрах этих команд используются следующие компоненты.

- Тип целевого объекта. Одно из predetermined значений, соответствующих классу объекта в Active Directory. Например: computer (компьютер), user (пользователь), OU (ОП), group (группа) и server (сервер, то есть контроллер домена).

- Идентификатор целевого объекта. *Различающееся имя* (distinguished name, DN) объекта, в отношении которого выполняется команда. DN объекта — это атрибут каждого объекта, представляющий его имя и местоположение в лесу Active Directory. Пример DN:

CN=Андрей Калиберда,OU=Employees,DC=povtas,DC=com

- Сервер. Можно указать контроллер домена, в отношении которого выполняется команда.

- Пользователь. Можно указать имя пользователя и пароль, с которыми следует выполнить команду.

Команда DSADD

Команда DSADD используется для создания объектов в Active Directory в определенном разделе каталога. Для создания объекта пользователя используйте команду DSADD USER. Параметры DSADD позволяют настраивать определенные свойства объекта. Можно создать пакетный файл с командами для создания множества объектов пользователей. Синтаксис команды DSADD для создания объектов пользователей имеет следующий вид:

dsadd user *DN_пользователя*.

Параметр *DN_пользователя* — это одно или несколько различающихся имен для создания новых объектов пользователей. Если DN содержит пробел, следует заключить всё имя в кавычки.

При использовании DSADD в интерактивном режиме из командной строки параметр *DN_пользователя* можно указать следующими способами:

- передавая по каналу списка DN_имен, полученного при выполнении другой команды (например, DSQUERY);
- указание всех DN_имен в командной строке через пробел;
- без указания параметра DN: вы сможете ввести все DN_имена по одному с клавиатуры в ответ на приглашение команды. Нажимайте Enter после ввода каждого DN. После ввода последнего DN нажмите Ctrl+Z и затем Enter.

Для команды DSADD USER после DN можно указывать необязательные параметры.

Так же следует добавить параметры *-s*, *-u* и *-p*, чтобы указать контроллер домена, для которого будет выполнена DSADD, а также имя и пароль пользователя, от имени которого будет выполняться эта команда:

- *{-s сервер | -d домен};*
- *-u имя пользователя;*
- *-p {пароль | *};*

Имя учетной записи SAM в значениях параметров *-email*, *-hmdir*, *-profile* и *-webpg* можно заменять специальной переменной *\$username\$* (не различает прописные и строчные буквы). Например, если имя учетной записи SAM равно *Andrey*, параметр *-hmdir* можно записать в любом из следующих форматов:

- *-hmdir\users\Andrey\home;*
- *-hmdir\users\\$username\$\home.*

Команда DSMOD

Команда DSMOD изменяет свойства одного или нескольких существующих объектов. Синтаксис команды имеет следующий вид:

dsmod user DN_пользователя [параметры].

Эта команда воспринимает параметр DN_пользователя точно так же, как команда DSADD, и для нее указываются те же параметры. Однако при помощи команды DSMOD USER нельзя изменять *имя_SAM* (параметр *-samid*) и членство в группах (параметр *-memberof*) объекта пользователя. Для изменения членства в группах из командной строки можно воспользоваться командой DSMOD GROUP.

Для команды DSMOD также можно указать параметр *-c*, который включает непрерывный режим DSMOD, когда команда выдает отчеты об ошибках, но продолжает модифицировать объекты. Если параметр *-c* не указан, DSMOD прекратит выполняться после первой ошибки.

Команда DSQUERY

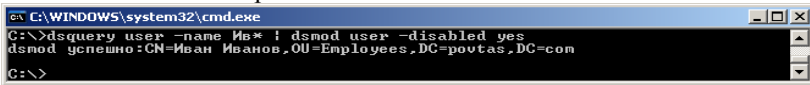
Команда DSQUERY запрашивает в Active Directory объекты, отвечающие указанному набору условий. Ее базовый синтаксис таков:

dsquery тип_объекта [{начальный_узел | forestroot | domainroot}] [-o {dn | rdn | samid}]

[-scope {subtree | onelevel | base}] [-name имя] [-desc описание] [-upn UPN] [-samid имя_SAM] [-inactive число_недель] [-stalepwd

число_дней] [-disabled] [{-s сервер|-d домен}] [-u имя_пользователя] [-p {пароль | *}]

Эта команда часто используется для генерации списка объектов, в отношении которых будут выполняться другие средства командной строки. Это достигается за счет пересылки по каналу выходных данных второй команде. Например, следующая команда запрашивает в Active Directory объект пользователя, имя которого начинается с «Ив» и передает набор результатов команде DSMOD, которая отключает все объекты из этого набора:



```

C:\WINDOWS\system32\cmd.exe
C:\>dsquery user -name Ив* ! dsmod user -disabled yes
dsmod успешно:CN=Иван Иванов,OU=Employees,DC=povtas,DC=com
C:\>

```

Прочие средства принимают на входе DN-имена, которые также являются выходным типом по умолчанию.

Основные параметры для команды DSQUERY перечислены ниже:

- **Тип_объекта.** Обязательный параметр. Тип объекта представляет класс(ы) объектов, среди которых будет производиться поиск. Можно указывать типы объектов computer (компьютер), contact (контакт), group (группа), OU (ОП), server (сервер), user (пользователь) или использовать групповой символ «*» для представления всех классов объектов.

- **Начальный_узел forestroot | domainroot.** Необязательный параметр. Указывает узел, с которого начинается поиск. Можно указать корень леса (forestroot), корень домена (domainroot) или различающееся имя узла (начальный_узел). Если задан корень леса, поиск будет выполняться в глобальном каталоге. Значение по умолчанию - domainroot.

- **-scope {subtree | onelevel | base}.** Задаёт область поиска. Значение subtree (поддерево) задаёт в качестве области поддерево с корнем в начальном узле. Значение onelevel (один уровень) задаёт поиск только в дочерних объектах первого уровня, считая от начального узла. Значение base (база) задаёт поиск в одном объекте, представленном как начальный узел. Если начальный_узел — forestroot (корень леса), единственная допустимая область поиска — subtree (поддерево). Область поиска по умолчанию — subtree.

- **-o {dn, rdn, samid}.** Определяет формат вывода списка записей, найденных в результате поиска. Значение dn задаёт отображение различающегося имени каждой записи. Значение rdn задаёт отображение относительного различающегося имени каждой записи.

Значение `samid` задает отображение имени учетной записи SAM (Security Accounts Manager) каждой записи. Формат по умолчанию — `dn`.

- **-name имя.** Ищет объекты пользователей, у которых атрибуты имени (значение атрибута `CN`) соответствуют имени. Можно использовать метасимволы.

- **-desc описание.** Ищет пользователей, атрибут описания которых соответствует значению описания. Можно использовать метасимволы.

- **-upn UPN.** Ищет пользователей, атрибут `UPN` которых совпадает с указанным `UPN`.

- **-samid имя_SAM.** Ищет пользователей, имя учетной записи SAM которых соответствует значению `имя_SAM`. Можно использовать метасимволы.

- **-inactive число недель.** Ищет всех пользователей, которые не входили в систему указанное количество недель.

- **-stalepwd число дней.** Ищет всех пользователей, которые не изменяли свои пароли в течение указанного количества дней.

- **-disabled.** Ищет всех пользователей, учетные записи которых отключены.

- **{-s сервер | -d домен}.** Подключается к указанному удаленному серверу или домену.

-u имя_пользователя. Задает имя пользователя для входа на удаленный сервер. По умолчанию параметр `-u` использует имя, под которым пользователь вошел в систему. Имя пользователя можно указать в любом из следующих форматов:

- имя пользователя (например `Andrey`);
- домен\имя пользователя (например, `bstu\Andrey`);
- имя участника_пользователя (`UPN`) (например

`Andrey@povtas.bstu.ru`).

- **-p {пароль \ *}.** Задает использование пароля или звездочки (*) для входа на удаленный сервер. Если вы введете *, появится окно с просьбой ввести пароль.

Команда DSGET

Команда `DSGET` получает и выводит выбранные свойства одного или нескольких существующих объектов. Ее базовый синтаксис таков:

`dsget user DN_пользователя [параметры].`

Эта команда воспринимает параметр `DN_пользователя` точно так же, как `DSADD`, и для нее указываются те же параметры, за исключением того, что `DSGET` принимает только параметр, но не связанное с ним значение. Например, `DSGET` поймет параметр `-samid`, но не пару, состоящую из параметра и значения: `-samid имя_SAM`. Кроме того, `DSGET` не поддерживает параметр `-password`, так как она не может отображать пароли.

Для `DSGET` можно указывать параметры `-dn` и `-sid`, которые отображают, соответственно, различающееся имя и `SID` объекта пользователя.

Команда **DSMOVE**

Команда `DSMOVE` предназначена для перемещения или переименования объекта в домене. Перемещать объекты между доменами при помощи этой команды нельзя. Ее базовый синтаксис таков:

```
dsmove DN_объекта [-newname новое_имя] [-newparent
DN_родителя]
```

`DSMOVE` также поддерживает параметры `-s`, `-u` и `-p`. Объект указывается по его различающемуся имени в параметре *DN объекта*. Чтобы переименовать объект, укажите для него новое обычное имя в параметре *новое_имя*. Если вы укажете различающееся имя контейнера в параметре *DN_родителя*, объект будет перемещен в этот контейнер.

Команда **DSRM**

Команда `DSRM` предназначена для удаления объекта, его поддерева или объекта вместе с поддеревом. Ее базовый синтаксис таков:

```
dsrcm DN_объекта [-subtree [-exclude]] [-noprompt] [-c].
```

`DSRM` поддерживает параметры `-s`, `-u` и `-p`, описанные в разделе, посвященном `DSQUERY`.

Объект указывается по его различающемуся имени в параметре `DN_объекта`. Параметр `-subtree` говорит `DSRM`, что, если объекты являются контейнерами, необходимо удалить их содержимое. Параметр `-exclude` исключает из рассмотрения сам объект, и его можно использовать только с параметром `-subtree`. Если указаны параметры `-subtree` и `-exclude`, то содержимое ОП и его поддерево будут удалены,

но ОП останется нетронутым. По умолчанию, если параметры -subtree или -exclude не указаны, удаляется только сам объект.

Удаление каждого объекта придется подтвердить, если только вы не зададите параметр -prompt. Параметр -s включает непрерывный режим DSRM, когда команда выдает отчеты об ошибках, но продолжает обрабатывать дополнительные объекты. Если параметр -c не указан, процесс прекратится после первой ошибки.

Управление профилями пользователей

Профиль пользователя представляет собой совокупность папок и файлов, содержащих элементы среды рабочего стола определенного пользователя. Профиль пользователя также содержит все элементы меню Пуск для данного пользователя, документы в папке Мои документы и список разрешенных сетевых дисков. Система автоматически создает профиль для каждого нового пользователя, впервые входящего на компьютер [4, 6].

По умолчанию профили пользователей хранятся локально на системном диске в папке %Systemdrive%\Documents and Settings\%Username%.

При первом входе пользователя, система создает для него профиль путем копирования профиля *Пользователь по умолчанию*. Имя для нового профиля формируется на основе имени для входа, указанного при первом входе в систему. Все изменения рабочего стола пользователя и программной среды хранятся в локальном профиле пользователя. Для каждого пользователя существуют отдельные профили, поэтому все параметры индивидуальны.

Пользовательская среда может быть расширена за счет профиля *Все пользователи*, который может включать ярлыки на рабочем столе или в меню Пуск, адреса компьютеров в сети и даже данные приложений. Для создания среды пользователя элементы профиля *Все пользователи* соединяются с профилем пользователя. По умолчанию только члены группы *Администраторы* могут модифицировать профиль *Все пользователи*.

Локальный профиль является локальным в полном смысле этого слова, т.е. если пользователь входит в другую систему, документы и параметры, являющиеся частью его профиля, не перемещаются. Вместо этого, когда пользователь впервые входит в систему, она генерирует для него новый локальный профиль.

Для поддержки пользователей, работающих на разных компьютерах, можно создать *перемещаемый профиль пользователя (RUP)*. Перемещаемые профили можно архивировать, проверять на

наличие вирусов и централизованно управлять ими. Даже в среде, где пользователи не перемещаются, RUP обеспечивает сохранность важной информации. Если система пользователя дала сбой и ее необходимо переустановить, RUP гарантирует, что новая пользовательская среда будет идентичная предыдущей. Чтобы настроить RUP, нужно создать общую папку на файловом сервере на котором часто проводится архивирование.

Чтобы пользователь работал с перемещаемым профилем, а не локальным, на вкладке Профиль диалогового окна Свойства пользователя следует ввести размещение профиля в поле *Путь к профилю* в следующем формате: `\\<имя_сервера>\<имя_общего_ресурса>% Username%`. Вместо переменной `% Username%` ОС автоматически подставляет имя входа пользователя. При следующем входе система найдет местоположение перемещаемого профиля и загрузит его.

Перемещаемый профиль пользователя это всего лишь общая папка и путь к папке профиля пользователя в пределах этого общего ресурса, указанный в свойстве объекта пользователя. При входе пользователя в систему создается локальная копия профиля на компьютере пользователя. Когда пользователь выходит из системы, его профиль выгружается на сервер профилей. При повторном входе пользователя на этот же компьютер система сравнивает локальную копию профиля с копией перемещаемого профиля на сервере и копирует только те компоненты профиля, которые были изменены. Поэтому вход и выход из системы с использованием RUP в Windows Server 2003 выполняется существенно быстрее, чем в предыдущих версиях Windows.

В Windows Server 2003 существует политика *Разрешать использование только локальных профилей*. Эта политика, связанная с ОП, содержащим учетные записи компьютеров, не позволяет использовать на данных компьютерах перемещаемые профили. Вместо этого пользователи работают с локальными профилями.

Обязательный профиль пользователя это перемещаемый профиль, доступный только для чтения. Он не позволяет пользователям изменять среду профиля и не сохраняет изменения от сеанса к сеансу. Пользователь получает настройки рабочего стола и других компонентов из обязательного профиля также как и из перемещаемого. Пользователь может изменять настройки, но все изменения после выхода из системы не сохраняются. При следующем входе в систему будут загружены те же настройки, что и в прошлый раз.

Обязательные профили полезны, если, создавая групповые профили, нужно чтобы изменения, которые внесет один пользователь, не повлияли на среду других пользователей.

Чтобы сделать профиль обязательным, следует переименовать файл Ntuser.dat в папке с перемещаемым профилем в Ntuser.man. Ntuser.dat - это скрытый файл с параметрами реестра, поэтому следует в программе *Свойства папки* из *Панели управления* включить параметр Показывать скрытые файлы и папки.

После настройки объектов пользователей перед администратором встают еще две проблемы: уязвимость, которая может привести к нарушению целостности сети всей организации, и вопросы из области инженерной психологии, связанные со стараниями сделать сеть и проверку подлинности в целом надежными и дружественными для пользователей. К сожалению, эти тенденции развиваются в противоположных направлениях: чем безопаснее сеть, тем неудобнее в ней работать.

Active Directory в Windows Server 2003 поддерживает политики безопасности, обеспечивающие сложность паролей и их безопасное использование в рамках предприятия. Необходимо разработать политику паролей, эффективно защищающую от злоумышленников, но в то же время удобную для пользователей, чтобы они не забывали свои пароли (иначе возрастет количество звонков в службу поддержки) или, что еще хуже, где-то записывали их.

Рядовой сервер под управлением Windows Server 2003 поддерживает политику для своих локальных учетных записей пользователей, которая настраивается из оснастки *Локальная политика безопасности*.

Политика учетных записей домена управляется посредством ОГП Default Domain Policy. Для изучения и модификации этой политики следует открыть консоль *Active Directory — пользователи и компьютеры*, затем выбрать узел домена и в меню *Действие* выбрать *Свойства*. Далее перейдите на вкладку *Групповая политика*. Первый ОГП в списке — это объект политики, который управляет политиками учетных записей домена. Выберите эту политику и щелкните кнопку *Изменить*. Откроется консоль *Редактор объектов групповой политики*, в окне которой будет выбрана политика Default Domain Policy.

Политика паролей

Политики паролей позволяют защищать сеть путем внедрения лучших методик управления паролями, проверенных практикой.

Политика паролей должна быть стойкой к атакам и удобной для пользователей одновременно. Политики паролей представлены ниже.

1. **Требовать неповторяемости паролей.** Если политика включена, Active Directory хранит список недавно использованных паролей и не разрешает пользователю задавать пароль из этого списка. Когда пользователю предлагается сменить пароль, он не может повторно ввести тот же пароль, то есть увеличить срок его действия. Эта политика включена по умолчанию, причем максимальное значение для нее равно 24. Во многих организациях задают значение 6 или 12.

2. **Максимальный срок действия пароля.** Эта политика определяет, когда пользователю необходимо сменить пароль. Неизменные или редко изменяемые пароли более уязвимы, и злоумышленники могут использовать их для доступа к сети под существующей учетной записью. Значение по умолчанию — 42 дня. Обычно в организациях пароль меняют каждые 30-90 дней.

3. **Минимальный срок действия пароля.** Когда пользователю необходимо сменить пароль, то, даже если включена история паролей, он может просто несколько раз изменить пароль, чтобы обойти требования и снова ввести исходный пароль. Данная политика предотвращает такую ситуацию, требуя, чтобы между сменами паролей проходило определенное количество дней. Администратор или сотрудник службы поддержки с соответствующими разрешениями может в любое время сменить пароль в Active Directory. Но пользователю запрещено менять пароль более одного раза в течение указанного в этом параметре периода времени.

4. **Минимальная длина пароля.** Эта политика задает минимальное количество символов в пароле. По умолчанию в пароле Windows Server 2003 должно быть 7 символов.

5. **Пароль должен отвечать требованиям сложности.** По умолчанию эта политика включена. Она включает правила (фильтры) для новых паролей. В Windows Server 2003 требования фильтра паролей по умолчанию следующие:

- пароль не должен быть основан на имени учетной записи пользователя;
- в пароле должно быть не менее 6 символов;
- пароль должен содержать символы следующих типов (минимум три):
 - заглавные алфавитные символы (A...Z);
 - строчные алфавитные символы (a...z);
 - арабские цифры (0...9);
 - не алфавитно_цифровые символы (например ! \$ # , %) .

.Изменение требований к длине и сложности паролей не влияет на существующие пароли. После включения этих политик изменения будут влиять только на новые учетные записи и изменяемые пароли.

Политика блокировки учетной записи

Блокировка учетных записей позволяет системе после нескольких неудачных попыток входа в систему решить, что злоумышленник пытается подобрать пароль, чтобы воспользоваться учетной записью, и в целях безопасности заблокировать эту учетную запись и пресечь дальнейшие попытки входа в систему. Доменные политики блокировки учетных записей определяют предел для неавторизованных входов в систему, то есть количество неудачных попыток за период времени и требования, выполнение которых позволит разблокировать учетную запись, — пользователю придется просто подождать или обратиться к администратору. Ниже перечислены политики блокировки учетной записи.

1. **Пороговое значение блокировки.** Задаёт количество неудачных попыток входа в систему, влекущее блокировку учетной записи. Допустимые значения — от 0 до 999. Если вы выберете слишком маленькое значение (допустим, три), учетные записи могут блокироваться из-за невнимательности. Если значение равно 0, учетные записи не блокируются никогда. Значение счетчика блокировки не изменяется при попытке входа в систему на заблокированных рабочих станциях.

2. **Блокировка учетной записи на.** Определяет период времени, который должен пройти после блокировки до того, как Active Directory автоматически разблокирует учетную запись пользователя. Эта политика не включается по умолчанию, и ее полезно использовать только в сочетании с политикой Пороговое значение блокировки. Хотя допустимыми являются значения от 0 до 99 999 минут, то есть около 10 недель, небольшие значения (от 5 до 15 минут) могут существенно снизить количество атак, причем пользователи, заблокированные по ошибке, не будут ' при этом испытывать серьезных неудобств. Если выбрано значение 0, пользователю придется обратиться к соответствующему администратору, который разблокирует учетную запись вручную.

3. **Сброс счетчика блокировки через.** Этот параметр указывает время, которое должно пройти после неудачной попытки входа в систему до того, как значение счетчика Account Lockout будет сброшено до 0. Допустимые значения — от 1 до 99 999 минут, причем

значение параметра должно быть меньше или равно продолжительности блокировки учетной записи.

Политики аудита

Аудит - это процесс отслеживания действий пользователей и занесения выбранных типов событий в журнал безопасности. Политика аудита определяет типы событий, которые требуется собирать. Для того чтобы сконфигурировать политики аудита, в редакторе управления групповыми политиками следует открыть узел Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Локальные политики/Политика аудита. Необходимо помнить, что по умолчанию параметр политики аудита, для рабочих станций установлен на «Не определено». После настройки политики аудита события будут заноситься в журнал безопасности. В общей сложности, можно настраивать девять политик аудита.

1. **Аудит входа в систему.** Политика определяет, будет ли операционная система пользователя, для компьютера которого применяется данная политика аудита, выполнять аудит каждой попытки входа пользователя в систему или выхода из нее. Например, при удачном входе пользователя на компьютер генерируется событие входа учетной записи. События выхода из системы создаются каждый раз, когда завершается сеанс вошедшей в систему учетной записи пользователя.

2. **Аудит доступа к объектам.** Политика выполняет аудит попыток доступа пользователей к объектам, которые не имеют отношения к Active Directory. К таким объектам можно отнести файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом. Аудит создается только для объектов, для которых указаны списки управления доступом, при условии, что запрашиваемый тип доступа и учетная запись, выполняющая запрос, соответствуют параметрам в данных списках.

3. **Аудит доступа к службе каталогов.** При помощи этой политики безопасности можно определить, будет ли выполняться аудит событий, указанных в системном списке контроля доступа, который можно редактировать в диалоговом окне «Дополнительные параметры безопасности» свойств объекта Active Directory. Аудит создается только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа и учетная запись, выполняющая запрос, соответствуют параметрам в данном списке.

4. Аудит изменения политики. Эта политика указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав пользователям, аудита, учетной записи или доверия.

5. Аудит изменения привилегий. Используя эту политику безопасности, можно определить, будет ли выполняться аудит использования привилегий и прав пользователей.

6. Аудит отслеживания процессов. Политика определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам.

7. Аудит системных событий. При помощи этой политики можно узнать, перегружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени.

8. Аудит событий входа в систему. При помощи этой политики аудита можно указать, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учетных данных. При использовании этой политики создается событие для локального и удаленного входа пользователя в систему. Члены домена и компьютеры, не входящие в домен, являются доверенными для своих локальных учетных записей. Когда пользователь пытается подключиться к общей папке на сервере, в журнал безопасности записывается событие удаленного входа, причем события выхода из системы не записываются.

9. Аудит управления учетными записями. При помощи этой политики можно определить, необходимо ли выполнять аудит каждого события управления учетными записями на компьютере. В журнал безопасности будут записываться такие действия как создание, перемещение и отключение учетных записей, а также изменение паролей и групп.

Важно отличать вход в систему под учетной записью и общий вход. Когда пользователь входит на рабочую станцию под доменной учетной записью, эта станция регистрирует событие входа, а контроллер домена — событие входа учетной записи. Когда пользователь подключается к общей папке на сетевом сервере, тот регистрирует событие входа, а контроллер домена — событие входа учетной записи.

После того как настроен аудит, журналы безопасности начинают заполняться сообщениями о событиях. Сообщения можно просмотреть, выбрав Безопасность в оснастке Просмотр событий и дважды щелкнув нужное событие.

Управление проверкой подлинности пользователей

Когда пользователи забывают свои пароли, перемещаются или отключаются, необходимо соответственно управлять объектами этих пользователей. Наиболее распространенные административные задачи, связанные с учетными записями пользователей, — это разблокирование учетной записи, смена пароля, отключение, включение, переименование и удаление объектов пользователей.

Политика блокировки учетных записей требует, чтобы при превышении предела неудачных попыток входа учетная запись пользователя блокировалась и в течение указанного периода времени или до разблокирования учетной записи администратором попытки входа в систему были невозможны.

Чтобы разблокировать учетную запись пользователя, щелкните объект пользователя и в меню *Действие* выберите *Свойства*. Перейдите на вкладку *Учетная запись* и снимите флажок *Заблокировать учетную запись*.

Если пользователь забыл пароль, необходима смена пароля. Для этого не требуется знать старый пароль пользователя. Просто щелкните объект пользователя и в меню *Действие* выберите *Смена пароля*. Дважды введите новый пароль, чтобы подтвердить изменение. Кроме того, общепринятая практика в таких случаях — установить флажок *Требовать смену пароля при следующем входе в систему*.

Изменения в штате могут потребовать отключения, включения и переименования объектов пользователей. Эти действия выполняются схожим образом. Щелкните объект пользователя и в меню *Действие* выберите нужную команду:

- отключение и включение — если пользователю в течение длительного периода времени не требуется доступ к сети, отключите его учетную запись, а когда пользователю снова потребуется войти в сеть, включите ее. Заметьте, что в зависимости от текущего состояния объекта в меню *Действие* вы увидите только одну из команд: *Отключить* или *Включить*;

- удаление — если пользователь уволился, а замены в скором времени не ожидается, удалите его объект. Помните, что, удалив пользователя, вы удалите сведения о его членстве в группах и (из-за удаления SID) его права и разрешения. Если вы затем создадите

объект пользователя с тем же именем, у него будет другой SID, и вам потребуется переназначить права, разрешения и группы;

- переименование — объект пользователя потребуется переименовать, допустим, если он изменил фамилию или уволился, но для него планируется замена, и вы хотите сохранить права, разрешения, сведения о членстве в группах и большинство свойств.

4. Учетные записи групп. Групповые политики

Понятие типа группы и области действия

Концепция группы, то есть именованного набора объектов, используется во многих системах. В частности, она характерна для систем безопасности, где в группы объединяются пользователи, которым назначены одинаковые разрешения или права. При поддержке данной концепции процесс предоставления разрешений пользователям значительно упрощается, поскольку назначить их сразу всей группе намного легче, чем каждому пользователю в отдельности.

Группы Active Directory — это гибкие структуры, которые могут включать объекты практически любых типов и используются для самых разных целей, в том числе для управления доступом пользователей к ресурсам и определения фильтров в случае применения групповых политик. Если разрешения безопасности для группы заданы в *таблице управления доступом* для некоего ресурса, то их получают все члены группы. Кроме того, группы Active Directory можно использовать в качестве списков рассылки сообщений электронной почты [1, 9, 10].

В Windows Server 2003 каждая группа имеет определенную область действия и относится к одному из двух типов: *безопасности* или *распространения*. Группы безопасности используются для ограничения доступа к ресурсам, а группы распространения — просто как механизм группировки объектов. Группу безопасности можно использовать в качестве группы распространения, но не наоборот. Правильное планирование структуры групп влияет на производительность и масштабируемость, особенно в корпоративных средах, содержащих множество доменов.

Область действия группы может быть *глобальной, универсальной* или *локальной доменной*. Она определяет, в какой части леса располагаются включаемые в группу объекты и в какой части леса группа используется в списках контроля доступа. Члены универсальных и локальных доменных групп могут относиться к любым доменам леса, но при этом первым разрешения обычно предоставляются в любом домене леса, а вторым — только в локальном. Глобальные группы включают пользователей из того же домена, к которому относится группа, но зато им могут быть предоставлены разрешения в любом домене леса [4, 6].

Локальные группы используются в основном для обратной совместимости с Windows NT4. На компьютерах с Windows Server

2003 существуют локальные пользователи и группы, сконфигурированные как рядовые серверы. Контроллеры доменов не используют локальные группы.

Локальные группы могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня и действуют в пределах конкретного компьютера и могут предоставлять разрешения для ресурсов только на этом компьютере.

Локальные группы домена главным образом используются для назначения глобальным группам разрешений на доступ к локальным ресурсам домена. Они существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном. Локальные группы домена доступны в пределах всего домена только в доменах основного режима Windows 2000 или доменах Windows Server 2003. Локальная группа домена функционирует подобно локальной группе на контроллере домена, пока домен работает в смешанном режиме. Локальная группа домена может содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня. Она действует в пределах домена в основном режиме Windows 2000 и режиме Windows Server 2003 и может использоваться для предоставления прав на ресурсы на любом компьютере с Windows Server 2003 в том домене, где определена группа.

Глобальные группы обычно используются для предоставления категоризированного членства в локальных группах доменов для отдельных участников безопасности и для прямого назначения разрешений. Часто глобальные группы применяются для объединения пользователей или компьютеров в одном домене и совместного исполнения одной работы, роли или функции. Они существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном, могут содержать только членов из своего домена, могут сами являться членами локальной группы компьютера или домена могут получать разрешения в любом домене, включая доверенные домены в других лесах и домены пред_Windows 2003. Глобальные группы могут содержать другие глобальные группы, но только в домене, работающем в основном режиме Windows 2000 или в режиме Windows Server 2003.

Универсальные группы в основном применяют для предоставления доступа к ресурсам во всех доверенных доменах. Однако такие группы могут использоваться только как участники безопасности (то есть как группы безопасности) в доменах, работающих в основном режиме Windows 2000 или в режиме Windows

Server 2003. Универсальные группы могут содержать участников из любого домена в лесу. В домене основного режима Windows 2000 или режима Windows Server 2003 универсальным группам могут предоставляться разрешения в любом домене, включая доверенные домены в других лесах. Универсальные группы помогают представить и объединить группы, которые распределены по разным доменам и выполняют типичные функции в рамках организации. Рекомендуется делать универсальными широко используемые и редко изменяемые группы.

Специальные группы

Существует несколько специальных групп, которые управляются самой ОС. Их нельзя создать, удалить или изменить их состав. Специальные группы не отображаются в консоли Active Directory — пользователи и компьютеры и другими средствами управления компьютером, однако им можно назначить разрешения в ACL ресурса.

Специальные группы и их представление описаны ниже:

- **Все.** Представляет всех пользователей сети, в том числе вошедших под гостевой учетной записью, а также пользователей из других доменов. Каждый раз при входе в систему пользователь автоматически добавляется в группу Все.

- **Сеть.** Представляет пользователей, которые в настоящий момент обращаются к данному ресурсу по сети (в отличие от тех, кто обращается к ресурсу локально). При любом обращении к данному ресурсу по сети пользователь автоматически добавляется эту в группу.

- **Интерактивные.** Представляет всех пользователей, которые локально обращаются к ресурсу (в отличие от тех, что обращаются к ресурсу по сети). При любом обращении к данному ресурсу пользователь автоматически добавляется в эту группу.

- **Анонимный вход.** В эту группу зачисляются те, кто использует сетевые ресурсы, не пройдя проверку подлинности.

- **Прошедшие проверку.** В эту группу входят все пользователи, которые прошли проверку подлинности при входе в сеть, предоставив действительную учетную запись. При назначении разрешений можно вместо Все использовать группу Прошедшие проверку, чтобы избежать анонимного доступа к ресурсам.

- **Создатель-владелец.** В эту группу зачисляется пользователь, который создал ресурс или получил право владения им. Например, если пользователь создал ресурс, но Администратор получил право

владения им, в группе Создатель-владелец будет указан Администратор.

- **Удаленный доступ.** В группу Удаленный доступ зачисляют всех, кто подключен к сети через коммутируемое соединение.

Создание объектов групп и управление ими

Обычно группы создают из консоли Active Directory — пользователи и компьютеры, ярлык которой расположен в группе программ Администрирование. В окне консоли нужно щелкнуть правой кнопкой в правой панели контейнера и выбрать Создать\Группа. Затем определите тип и область действия создаваемой группы.

В домене смешанного или промежуточного режима группа безопасности может быть только глобальной или локальной группой домена. В таком домене нельзя создать группу безопасности с универсальной областью действия.

Впрочем, локальную группу домена, глобальную или универсальную группу в доменах смешанного или промежуточного режима можно создать в виде группы распространения. Группы безопасности в таком домене могут иметь локальную доменную или глобальную область действия.

Добавление или удаление членов группы также выполняется из консоли Active Directory — пользователи и компьютеры. Щелкните правой кнопкой любую группу и выберите *Свойства*. В табл. 4.1 описаны вкладки этого окна свойств для настройки членства.

Табл. 4.1. Настройка членства

Вкладка	Назначение
Члены группы	Добавление, удаление и отображение списка участников безопасности — членов этого контейнера
Член групп	Добавление, удаление и отображение перечня контейнеров, членом которых является данный контейнер

К средствам командной строки службы каталогов для просмотра и изменения состава группы относятся DSQUERY, DSGET, DSMOD и DSGROUP. Команда DSGET особенно удобна для получения списка всех групп, членом которых является пользователь.

Также служба каталогов Active Directory предоставляет гибкий и удобный механизм вложения групп. Глобальные группы могут быть вложены в другие глобальные, универсальные группы или локальные группы домена. Универсальные группы могут участвовать в других универсальных группах или локальных группах домена. Локальные группы домена могут участвовать в других локальных группах домена.

Вместе с тем, такая гибкость повышает сложность, и без соответствующих инструментов было бы трудно точно определить, к каким группам принадлежит пользователь. В Windows Server 2003 есть команда DSGET, которая решает эту проблему. Из командной строки исполните следующую команду:

```
dsget user DN_пользователя -memberof [-expand]
```

Параметр -memberof возвращает значение атрибута MemberOf и позволяет увидеть, к каким группам явно принадлежит пользователь. Добавив параметр -expand, можно провести рекурсивный поиск в группах и получить исчерпывающий список всех групп в домене, к которым принадлежит пользователь.

Автоматизация управления учетными записями групп

LDIFDE — это средство командной строки, доступное во всех редакциях Windows Server 2003. LDIFDE запускается из командной строки или командной оболочки с подходящими параметрами. Полный перечень параметров можно просмотреть, исполнив в командной строке `ldifde /?`. Формат LDIF можно использовать для массового экспорта и импорта данных, например для добавления, создания и изменения элементов в каталоге Active Directory

Часто приходится иметь дело с набором данных, уже содержащим часть информации, которую вы хотели бы поместить в Active Directory. Эти данные могут находиться в домене более низкого уровня или в базе данных иного типа (например, в БД отдела кадров).

Если имеются данные о пользователях, можно загрузить их в Active Directory. Существует много средств, облегчающих извлечение данных, например Addusers для Windows NT 4 или LDIFDE для Windows 2000. Кроме того, в большинстве СУБД имеются средства экспорта данных в файл с разделителями — запятыми (Comma-Separated-Value, CSV), который затем можно импортировать командой LDIFDE. Некоторые элементы обязательны для создания объекта и их отсутствие в таком файле вызовет ошибки импорта. Впрочем, для создания группы требуется знать лишь ее различающееся имя (CN=User) и местоположение (DC=Domain, DC=OU).

Создание групп командой DSADD

Для добавления группы используется следующий синтаксис:

`dsadd group DN_группы...`

Параметр `DN_группы...` задает одно или несколько различающихся имен для новых объектов групп. Если в `DN` есть пробел, следует заключить все имя в кавычки. Параметр `DN_группы...` можно вводить следующими способами.

1. Передача по каналу списка `DN_имен`, полученного при выполнении другой команды, например `DSQUERY`.

2. Указание всех `DN_имен` в командной строке через пробел.

3. Без указания параметра `DN`: тогда можно ввести все `DN_имена` по одному с клавиатуры в ответ на приглашение команды. Нажимайте `Enter` после ввода каждого `DN`. Нажмите `Ctrl+Z` и `Enter` после ввода последнего `DN`.

Для команды `DSADD GROUP` после `DN` можно указать следующие параметры:

`-secgrp {yes | no}` указывает тип группы: безопасности (`yes`, значение по умолчанию) или распространения (`no`);

`-scope {l | g | u}` определяет, является ли группа локальной в домене (`l`), глобальной (`g`, значение по умолчанию) или универсальной (`u`);

`-samid имя_SAM`;

`-desc описание`;

`-memberof DN_группы...` указывает группу, в которую надо добавить новую группу;

`-members DN_члена...` указывает различающиеся имена членов, которые будут добавлены в группу.

Так же можно добавить параметры `-s`, `-u` и `-p`, чтобы указать контроллер домена, для которого будет выполнена `DSADD`, а также имя и пароль пользователя (реквизиты), с которыми будет выполняться эта команда.

Изменение групп командой DSMOD

Команда `DSMOD`, изменяет объекты в Active Directory.

Для изменения группы используется следующий синтаксис:

`dsmod group DN_группы...`

Эта команда принимает многие параметры, используемые в `DSADD`, в том числе `-samid`, `-desc`, `-secgrp` и `-scope`. Наиболее полезные параметры:

- `-addmbr DN_члена_группы...` добавляет членов в группу, указанную в параметре `DN_группы`;

- `-rmmbr DN_члена_группы...` удаляет членов из группы, указанной в параметре `DN_группы`

Здесь `DN` обозначает полное различающееся имя другого объекта Active Directory (если в имени есть пробелы, заключите его в кавычки).

В вызове команды `DSMOD GROUP` можно использовать `-addmbr` или `-rmmbr`. Нельзя использовать оба этих параметра в команде `DSMOD GROUP`.

Перечень наиболее важных атрибутов объекта `group` приведен в табл. 4.2.

Таблица 4.2. Атрибуты объекта `group`

Атрибут	Описание
<code>cn</code>	Относительное отличительное имя объекта <code>group</code>
<code>createTimestamp</code>	Дата и время создания объекта
<code>description</code>	Текстовое описание группы
<code>groupType</code>	Набор флагов, определяющих область действия и тип группы
<code>info</code>	Дополнительная информация о группе
<code>primaryGroupToken</code>	Локальный RID группы. Он соответствует значению атрибута <code>primaryGroupID</code> объектов <code>user</code> , для которых данная группа является основной
<code>managedBy</code>	Относительное имя пользователя или группы, которая является владельцем данной группы
<code>managedObjects</code>	Список отличительных имен объектов <code>group</code> , в атрибуте <code>managedBy</code> которых указана данная группа
<code>member</code>	Список отличительных имен членов группы
<code>memberOf</code>	Список отличительных имен групп, членом которых является данная группа
<code>modifyTimestamp</code>	Дата и время последнего изменения группы
<code>sAMAccountName</code>	Имя учетной записи SAM данной группы. Обычно совпадает со значением атрибута <code>cn</code>
<code>wWWHomePage</code>	URL домашней страницы группы

Управление группами с помощью сценариев

Нижеследующий код создает глобальную группу безопасности.

```
' ----- SCRIPT CONFIGURATION -----'
```

```

    strGroupParentDN = "<ОИ_род_объекта_группы>" ' Например:
ou=Groups,dc=povtas,dc=com
    strGroupName = "<имя_группы>" ' Например:
ExecAdminsSales
    strGroupDescr = "<описание_группы>" ' Например:
Executive Admins for Sales group
' ----- END CONFIGURATION -----

```

```

' Constants taken from ADS_GROUP_TYPE_ENUM
Const ADS_GROUP_TYPE_DOMAIN_LOCAL_GROUP = 1
Const ADS_GROUP_TYPE_GLOBAL_GROUP = 2
Const ADS_GROUP_TYPE_LOCAL_GROUP = 4
Const ADS_GROUP_TYPE_SECURITY_ENABLED =
-2147483648
Const ADS_GROUP_TYPE_UNIVERSAL_GROUP = 8

set objOU = GetObject("LDAP://" & strGroupParentDN)
set objGroup = objOU.Create("group","cn=" & strGroupName)
objGroup.Put "groupType", ADS_GROUP_TYPE_LOCAL_GROUP _
Or ADS_GROUP_TYPE_SECURITY_ENABLED
objGroup.Put "sAMAccountName", strGroupName
objGroup.Put "description", strGroupDescr
objGroup.SetInfo

```

В приведенном выше сценарии создается группа, не содержащая ни одного члена. В атрибуте groupType содержится набор флагов, определяющих область действия и тип группы. Значения этих флагов указаны в перечислении ADS_GROUP_TYPE_ENUM.

Для просмотра списка непосредственных членов группы используется следующий сценарий.

```

' ----- SCRIPT CONFIGURATION -----
    strGroupDN = "<ОИ_группы>" ' Например:
cn=SalesGroup,ou=Groups,dc=povtas,dc=com
' ----- END CONFIGURATION -----

```

```

set objGroup = GetObject("LDAP://" & strGroupDN)
Wscript.Echo "Members of " & objGroup.Name & ":"
for each objMember in objGroup.Members
    Wscript.Echo objMember.Name
next

```

Атрибут member объекта group содержит отличительные имена непосредственных членов группы. Употребляя данное понятие,

имеется в виду напрямую добавленные в группу объекты (но не объекты, входящие в ее вложенные группы).

Для просмотра списка косвенных членов группы служит следующий сценарий.

```
' ----- SCRIPT CONFIGURATION -----
strGroupDN = "<ОИ_группы>" ': cn=SalesGroup, ou=Groups,
dc=povtas, dc=com
' ----- END CONFIGURATION -----
strSpaces = " "
set dicSeenGroupMember = CreateObject("Scripting.Dictionary")
Wscript.Echo "Members of " & strGroupDN & " ."
DisplayMembers "LDAP://" & strGroupDN, strSpaces,
dicSeenGroupMember
Function DisplayMembers (strGroupADsPath, strSpaces,
dicSeenGroupMember)
set objGroup = GetObject(strGroupADsPath)
for each objMember In objGroup.Members
    Wscript.Echo strSpaces & objMember.Name
    if objMember.Class = "group" then
        if dicSeenGroupMember.Exists(objMember.ADsPath)
then
            Wscript.Echo strSpaces & " ^already seen group
member "&
                                "(stopping to avoid
loop)"
        else dicSeenGroupMember.Add objMember.ADsPath, 1
            DisplayMembers objMember.ADsPath, strSpaces & "
",
                                dicSeenGroupMember
        end if
    end if
next
End Function
```

Список членов группы хранится в составном атрибуте member объекта group. Однако этот атрибут содержит только имена непосредственных членов группы, а имена членов ее вложенных групп в нем отсутствуют. Для того чтобы их получить, необходимо рекурсивно просмотреть списки членов каждой из вложенных групп.

В приведенном выше сценарии на языке VBScript используется объект-словарь dictionary, куда записывается список всех членов

текущей обрабатываемой группы. Перед вызовом функции DisplayMembers проверяется, обрабатывалась ли уже данная группа. Если она обрабатывалась, выводится соответствующее сообщение. Подобная проверка необходима в случае циклической вложенности групп, когда, к примеру, группа А входит в группу Б, группа Б — в группу В, а группа В — в группу А.

Для добавление или удаления членов группы используется следующий сценарий.

```
' ----- SCRIPT CONFIGURATION -----
StrGroupDN = "<ОИ_группы>"      ' Например:
cn=SalesGroup,ou=Groups,dc=povtas,dc=com
strMemberDN = "<ОИ_члена>"      ' Например:
cn=petr.petrov,cn=users,dc=povtas,dc=com
' -----END CONFIGURATION-----

set objGroup = GetObject("LDAP://" & strGroupDN)
' Add a member
objGroup.Add("LDAP://" & strMemberDN)

' Этот код удаляет объект из группы
' ----- SCRIPT CONFIGURATION -----
StrGroupDN = "<ОИ_группы>"      ' Например:
cn=SalesGroup,ou=Groups,dc=povtas,dc=com
strMemberDN = "<ОИ_члена>"      ' Например:
cn=petr.petrov,cn=users,dc=povtas,dc=com
' -----END CONFIGURATION-----

set objGroup = GetObjec("LDAP://" & strGroupDN)
' Удаление
objGroup.Remove("LDAP://" & strMemberDN)
```

Поскольку в атрибут member можно помещать любые отличительные имена, членами группы могут быть любые объекты. И если организационные подразделения обычно используются для объединения объектов на основе некоторого критерия, с помощью объектов group можно группировать разнородные объекты.

Один и тот же объект может быть членом нескольких групп, что нехарактерно для подразделений, поэтому в отдельных случаях для группировки объектов в большей мере подходят группы, нежели подразделения. Еще одной важной особенностью групп является то обстоятельство, что им можно назначать разрешения на доступ к

ресурсам, поскольку в Active Directory они являются участниками системы безопасности, тогда как подразделения к числу таковых не относятся. В некоторых других службах каталогов, например в Novel Netware, подразделения также выступают участниками системы безопасности.

Для перемещения группы используем сценарий, который подходит для перемещения любого объекта.

В пределах домена:

```
' Этот код перемещает объект в другое место в пределах домена
' ----- SCRIPT CONFIGURATION -----
strNewParentDN = "LDAP://<ОИ_нового_контейнера>"
strObjectDN    = "LDAP://cn=petr.petrov,
<ОИ_старого_контейнера>"
strObjectRDN   = "cn=petr.petrov"
' ----- END CONFIGURATION -----
set ObjCont = GetObject(strNewParentDN)
objCont.MoveHere strObjectDN, strObjectRDN
```

Прежде всего, для нового родительского контейнера необходимо вызвать метод `GetObject`. Получив ссылку на представляющий его объект, вызываем для него метод `MoveHere`, задав в первом параметре значение атрибута `AOsPath` перемещаемого объекта, а во втором — отличительное имя этого объекта. Элемент `cn=petr.petrov` задается в параметрах метода `MoveHere` дважды, потому что указанный метод может использоваться не только для перемещения, но и для переименования объектов.

В другой домен:

```
set objObject = GetObject("LDAP://TargetDC/TargetParentDN")
objObject.MoveHere "LDAP://SourceDC/SourceDN", vbNullString
В следующем примере объект cn = petr.petrov из домена
amer.povtas.com перемещается в домен emea.povtas.com
set objObject = GetObject("LDAP://dc-
amer1/cn=users,dc=amer,dc=povtas,dc=com")
objObject.MoveHere "LDAP://dc-
emea1/cn=jsmith,cn=users,dc=emea,dc=povtas,dc=com", vbNullString
```

Перемещение объектов между разными доменами выполняется в соответствии с приведенными ниже правилами:

- Пользователь, желающий переместить объекты, должен иметь разрешения на их изменение в родительских контейнерах обоих доменов;
- Нужно явно указать целевой контроллер домена;
- Операция перемещения должна выполняться на хозяине RID обоих доменов;
- Оба домена должны работать в основном режиме Windows 2000;
- При перемещении объекта user в другой домен идентификатор этого объекта objectSID заменяется новым идентификатором, а старый SID добавляется в атрибут SIDHistory;
- Из объектов типа group можно перемещать только универсальные группы. Чтобы переместить глобальную группу или локальную группу домена, сначала нужно преобразовать ее в универсальную.

Между доменами разрешается перемещать только универсальные группы. Если нужно переместить в другой домен глобальную группу или локальную группу домена, то таковую вначале нужно преобразовать в универсальную, а после перемещения вернуть ее исходный тип. Однако при попытке преобразовать группу в группу другого типа можно столкнуться с проблемами, обусловленными теми ограничениями, которые налагаются на членство в группах разных типов.

Перемещение группы между доменами проще всего выполнить с помощью специальной утилиты ADMT (Active Directory Migration Tool - средство миграции Active Directory). Она позволяет перемещать и реструктурировать группы без их преобразования из одного типа в другой и без изменения списка или разрешений их членов.

Для изменения области действия и типа группы используется следующий сценарий.

```
' ----- SCRIPT CONFIGURATION -----
strGroupDN = "<ОИ_группы>" ' Например:
cn=SalesGroup,ou=Groups,dc=povtas,dc=com
' ----- END CONFIGURATION -----
' Константы из ADS_GROUP_TYPE_ENUM
ADS_GROUP_TYPE_DOMAIN_LOCAL_GROUP = 1
ADS_GROUP_TYPE_GLOBAL_GROUP      = 2
ADS_GROUP_TYPE_LOCAL_GROUP        = 4
```

```

ADS_GROUP_TYPE_SECURITY_ENABLED = -2147483648
ADS_GROUP_TYPE_UNIVERSAL_GROUP = 8
set objGroup = GetObject("LDAP://" & strGroupDN )
objGroup.Put "groupType",
ADS_GROUP_TYPE_UNIVERSAL_GROUP
Or ADS_GROUP_TYPE_SECURITY_ENABLED
objGroup.SetInfo

```

Информация об области действия и типе группы записывается в виде флагов в атрибуте groupType объекта group. Для непосредственной установки значения этого атрибута нужно объединить устанавливаемые флаги с помощью логической поразрядной операции OR. Для группы распространения не существует специальной константы, которая определяла бы тип группы. Поэтому при необходимости задать группу распространения просто не нужно включать в формируемое значение атрибута groupType константу ADS_GROUP_TYPE_SECURITY_ENABLED.

5. Учетные записи компьютеров

В стандартной конфигурации Windows Server 2003 и всех ОС Microsoft Windows компьютер принадлежит какой-либо *рабочей группе*. В рабочей группе компьютер на базе Windows NT (включая Windows NT 4, 2000, XP и Windows Server 2003) может проверять подлинность пользователей только из своей локальной БД *диспетчера учетных записей безопасности*. Принадлежность к рабочей группе позволяет лишь видеть список компьютеров своей группы в *Проводнике*. Хотя пользователь такого компьютера и может подсоединяться к общим ресурсам на других машинах в рабочих группах или доменах, он на самом деле не входит в систему под доменной учетной записью.

Чтобы пользователь входил в систему под доменной учетной записью, компьютер должен принадлежать домену. Для этого необходимо создать учетную запись компьютера и настроить его для присоединения к домену по этой учетной записи.

Учетная запись компьютера содержит имя, пароль и *идентификатор безопасности*. Эти свойства встроены в класс объекта компьютера в Active Directory. Для включения компьютера в домен, сначала нужно создать в Active Directory объект компьютера [1, 5, 9].

Создание учетных записей компьютеров

Для создания объекта компьютера в Active Directory необходимо быть членом групп *Администраторы* или *Операторы учета* на контроллерах домена. Кроме того можно делегировать административные права, чтобы другие пользователи или группы могли создавать объекты компьютеров.

Пользователи домена также могут создавать объекты компьютеров косвенным путем. Когда компьютер присоединяется к домену, а учетная запись еще не создана, Active Directory по умолчанию автоматически создает объект компьютера в контейнере Computers. Каждому пользователю из группы *Прошедшие проверку* (то есть всем пользователям) разрешается присоединять к домену до 10 компьютеров и, следовательно, создавать до 10 объектов компьютеров.

Объект компьютера должен создаваться до его присоединения к домену. Существует несколько способов создания объекта компьютера.

Первый способ. Откройте консоль *Active Directory — пользователи и компьютеры* и выберите контейнер или ОП, в котором нужно создать объект. В меню Действие или в контекстном меню выберите команду Создать\Компьютер. Откроется диалоговое окно Новый объект — Компьютер, показанное на рис. 5.1. В окне Новый объект — Компьютер введите имя компьютера. Щелкните ОК.

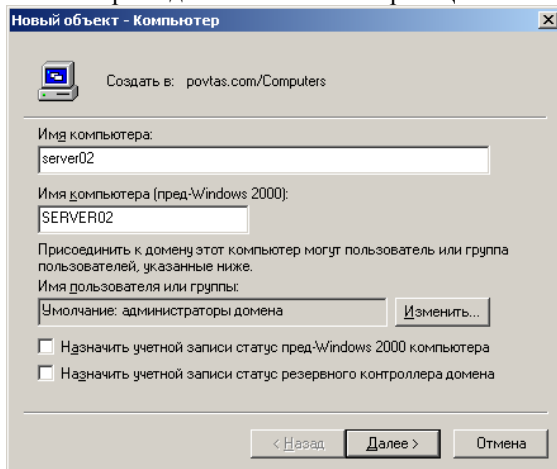


Рис. 5.1. Диалоговое окно *Новый объект — Компьютер*

Второй способ. С помощью команды DSADD. Она позволяет создавать объекты компьютеров из командной строки или в ходе выполнения командного файла.

Для создания объекта компьютера введите `dsadd computer DN_компьютера`,

где *DN_компьютера* — это различающееся имя данного компьютера, например `CN=Server2,OU=Desktops,DC=povtas,DC=com`.

Если в DN компьютера есть пробел, нужно заключить все имя в кавычки. Параметр *DN_компьютера...* может включать множество различающихся имен для новых объектов компьютеров, что делает команду DSADD Computer удобным средством для массовой генерации таких объектов. Этот параметр можно вводить следующими способами:

- передача по каналу списка DN-имен, полученного при выполнении другой команды, например DSQUERY;
- указание всех DN-имен в командной строке через пробел;
- без указания параметра DN: тогда можно ввести все DN-имена по одному с клавиатуры в ответ на приглашение команды. Нажимайте

Enter после ввода каждого DN. Нажмите Ctrl+Z и затем Enter после ввода последнего DN.

Третий способ. Создание учетной записи компьютера командой NETDOM, которая входит в комплект средств поддержки и устанавливается из каталога Support\Tools компакт-диска Windows Server 2003. Эта программа также содержится на компакт-дисках Windows 2000 и XP. Команда NETDOM позволяет выполнять из командной строки множество операций, связанных с учетными записями доменов и безопасностью.

Синтаксис NETDOM с параметром add следующий:

netdom add

имя_компьютера/domain:имя_домена/userd:пользователь/PasswordD:
пароль_пользователя [/ou:DN_ОП]

Эта команда создает учетную запись для компьютера *имя_компьютера* в домене *имя_домена* от имени *пользователя* домена с паролем *пароль_пользователя*. Параметр /ou приводит к созданию объекта в ОП с различающимся именем *DN_ОП*. Если имя целевого ОП не указано, по умолчанию учетная запись компьютера создается в контейнере Computers. Инициатор команды должен обладать разрешениями на создание объектов компьютеров.

Присоединение компьютера к домену

Учетной записи компьютера в AD недостаточно для создания необходимых безопасных отношений между доменом и компьютером. Компьютер нужно присоединить к домену. Порядок присоединения следующий:

1. Щелкните правой кнопкой Мой компьютер и выберите Свойства (Properties). Перейдите на вкладку Имя компьютера. В *Панели управления* выберите Система и в диалоговом окне Свойства системы перейдите на вкладку Имя компьютера. Откройте окно свойств Имя компьютера. К свойствам компьютера на этой вкладке можно получить доступ несколькими способами. В Windows 2000 вкладка Имя компьютера называется Сетевая идентификация, а кнопка Изменить - Свойства.

2. В *Панели управления* откройте Сетевые подключения и в меню Дополнительно выберите Сетевая идентификация.

3. На вкладке Имя компьютера щелкните кнопку Изменить. Диалоговое окно Изменение имени компьютера позволяет изменить имя компьютера и его принадлежность к домену и рабочей группе (рис. 5.2).

4. В окне Изменение имени компьютера установите переключатель в положение домена и введите нужное имя домена.

5. Щелкните ОК. Компьютер попытается связаться с контроллером домена. Если связаться с доменом не удастся, нужно проверить сетевые подключения и их параметры, а также конфигурацию DNS.

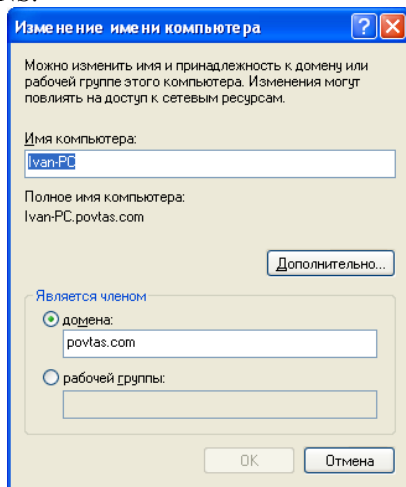


Рис. 5.2. Диалоговое окно *Изменение имени компьютера*

Когда компьютер успешно свяжется с доменом, появится приглашение (рис. 5.3) для ввода имени пользователя и пароля, у которого есть привилегии присоединять компьютер к домену.

Если в домене заранее не была создана учетная запись компьютера с тем же именем, по умолчанию Active Directory автоматически создаст такую учетную запись в контейнере Computers. После того как доменная учетная запись компьютера найдена или создана, компьютер установит доверительные отношения с доменом, изменит свой SID, чтобы он совпадал с SID этой доменной учетной записи, и изменит свое членство в группах. Для завершения процесса компьютер необходимо перезагрузить.

Для присоединения рабочей станции или сервера к домену также можно применять команду NETDOM JOIN. Ее функции идентичны возможностям диалогового окна Изменение имени компьютера, и она позволяет задать еще и ОП, в котором будет создана учетная запись, если соответствующего объекта компьютера еще нет в Active Directory.

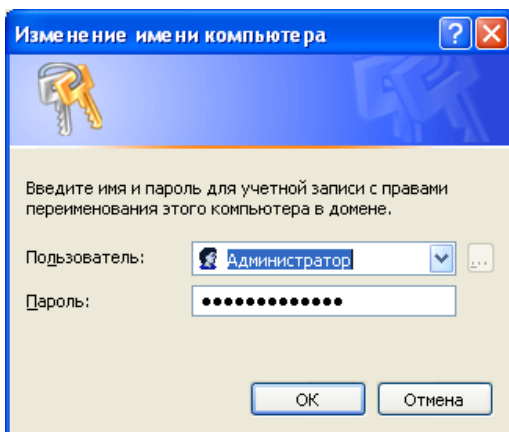


Рис. 5.3. Запрос реквизитов для присоединения компьютера к домену

По умолчанию Active Directory помещает объекты компьютеров в контейнер Computers. Если к домену присоединяется компьютер, для которого в этом домене еще нет учетной записи, объект компьютера создается автоматически.

Такие контейнеры, как Computers, Users и Builtin не могут быть связаны с политиками, ограничивающими возможную область действия групповой политики в отношении компьютеров. Поэтому стоит включить в структуру Active Directory минимум одно ОП для компьютеров. Обычно для компьютеров создают несколько ОП на основании структуры организации, местоположения компьютеров или назначения ОП, чтобы можно было отдельно администрировать ноутбуки, рабочие станции, серверы файлов, печати или приложений.

Если в организации создано одно или несколько ОП для компьютеров, придется перемещать все объекты компьютеров, автоматически создаваемые в контейнере Computers, в соответствующие ОП. Для перемещения нужно отметить компьютер и в меню Действие выберите Переместить. Кроме того, для перемещения можно использовать новую функцию перетаскивания (drag-and-drop) объектов, поддерживаемую MMC.

Т.к. никакой объект компьютера в контейнере Computers не управляется групповыми политиками для ОП, выделенных для компьютеров, и т.к. необходимы дополнительные действия по переносу объекта компьютера из контейнера Computers в соответствующее ОП, рекомендуется создавать объекты компьютеров до присоединения к домену. Можно сначала создать объект

компьютера в нужном ОП, чтобы сразу после присоединения к домену он управлялся политиками, связанными с данным ОП.

Можно также перемещать объект компьютера или любой другой объект командой DSMOVE. Ее синтаксис следующий:

```
dsmove DN_объекта [-newname новое_имя] [-newparent
DN_родителя]
```

Параметр -newname для переименования объекта. Параметр -newparent для перемещения объекта. Для перемещения компьютера Ivan-PC из контейнера Computers в ОП Desktops нужно ввести следующую команду:

```
dsmove "CN=Ivan-PC, CN=Computers, DC=povtas, DC=com" –
newparent "OU=Desktops, DC=povtas, DC=com"
```

Для перемещения объектов в Active Directory необходимы соответствующие разрешения. По умолчанию членам группы *Операторы учета* разрешается перемещать компьютеры между контейнерами, включая контейнер Computers, и любыми ОП, за исключением ОП Domain Controllers. Администраторы, включая членов групп *Администраторы домена* и *Администраторы предприятия*, вправе перемещать объекты компьютеров между любыми контейнерами, включая контейнер Computers, ОП Domain Controllers и любые другие ОП.

Управление разрешениями для объекта компьютера

Active Directory позволяет определить, какие группы или пользователи могут сопоставлять компьютер его доменной учетной записи. По умолчанию такой группой является *Администраторы домена*, но присоединять компьютер к доменной учетной записи можно разрешить любой группе. Легче всего это делать во время создания объекта компьютера.

При создании объекта компьютера на первом шаге в окне Новый объект — Компьютер, показанном на рис. 5.1, отображается поле Присоединить к домену этот компьютер могут пользователь или группа пользователей, указанные ниже. Щелкните Изменить, и вы сможете выбрать любого пользователя или группу и изменить для данного объекта набор разрешений.

Если компьютер, который будет использовать создаваемую учетную запись, работает под управлением версии Windows младше 2000, установите флажок Назначить учетной записи статус пред-Windows 2000 компьютера. Если эта учетная запись предназначена для

резервного контроллера домена Windows NT, установите флажок Назначить учетной записи статус резервного контроллера домена.

Принадлежать домену могут только компьютеры, на которых установлена ОС на основе технологий Windows NT, поэтому компьютеры под управлением Windows 9x/Me не могут присоединяться к доменным учетным записям компьютеров или обрабатывать их. Поэтому данный флажок фактически подразумевает наличие Windows NT 4.

Настройка свойств объекта компьютера

Объекты компьютеров обладают некоторыми свойствами, которые не отображаются в пользовательском интерфейсе во время создания учетной записи компьютера. Откройте окно свойств для объекта компьютера, чтобы задать его расположение и описание, настроить членство в группах и разрешение удаленного доступа или связать его с объектом пользователя — владельцем данного компьютера. Страница свойств Операционная система доступна только для чтения. Эта информация публикуется в Active Directory автоматически. Данная страница остается незаполненной, пока компьютер не присоединится к домену по этой учетной записи.

Несколько классов объектов в Active Directory поддерживают свойство Manager, которое отображается на странице Управляется в окне свойств объекта компьютера. Это связанное свойство создает перекрестную ссылку на объект пользователя.

Все остальные свойства (адреса и номера телефонов) не хранятся в самом объекте компьютера, а берутся напрямую из этого объекта пользователя.

С помощью команды DSMOD можно изменять некоторые свойства объекта компьютера.

Поиск и подключение к объектам в Active Directory

При обращении пользователя может понадобиться информация о том, какая ОС и какой пакет обновления установлены на его компьютере. Эта информация хранится в свойствах объекта компьютера. Остается только найти этот объект, что, впрочем, может быть просто в структуре Active Directory с несколькими именами и множеством ОП.

Консоль *Active Directory — пользователи и компьютеры* предоставляет удобный доступ к мощному средству поиска с графическим интерфейсом. Это средство позволяет находить объекты многих типов. Для того, чтобы найти объект типа Computer, щелкните

кнопку Поиск объектов в службе каталогов Active Directory на панели инструментов консоли. Откроется окно, показанное на рис. 5.4. Перед тем как щелкнуть Найти, вы можете выбрать тип объекта в списке Найти, область поиска в списке и указать условия поиска.

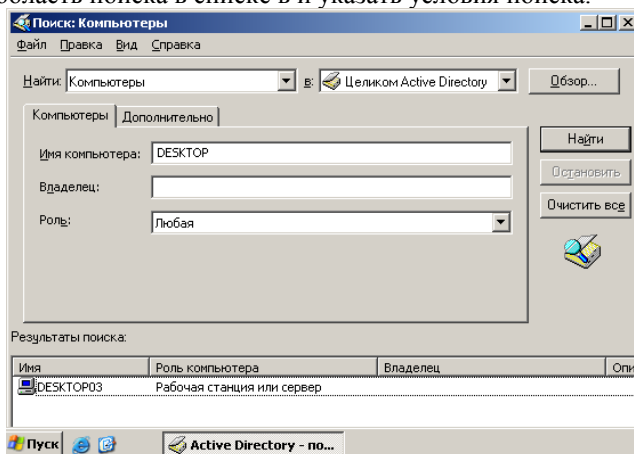


Рис. 5.4. Диалоговое окно *Поиск: Компьютеры*

Перечень результатов позволяет выбрать объект и посредством меню Файл или контекстного меню выполнить с выделенным объектом типичные операции. Многим администраторам нравится возможность открыть консоль *Управление компьютером* по команде Управление контекстного меню и напрямую подключиться к этому компьютеру, после чего работать на нем с журналами событий, диспетчером устройств, информацией о системе, конфигурациями дисков и служб, а также локальными учетными записями пользователей и групп.

Устранение неполадок с учетными записями компьютеров

У компьютера, как и у пользователя, есть учетная запись, или, свойства объекта компьютера: имя, пароль и SID.

Учетные записи компьютеров обладают уникальным SID, позволяющим администратору предоставлять разрешения компьютерам. Компьютеры можно включать в группы. Когда учетная запись компьютера удаляется, его членство в группах и SID теряются. Если удаление было случайным, и с этим именем создается другая учетная запись компьютера, это будет совершенно новая учетная запись с новым SID. Отношения с группами потребуется восстановить, и все

разрешения, назначенные удаленному объекту компьютера, необходимо переназначить новой учетной записи.

Для удаления учетной записи компьютера в оснастке *Active Directory — пользователи и компьютеры* щелкните нужный объект компьютера, а затем в меню Действие или в контекстном меню выберите Удалить. Вас попросят подтвердить удаление, и, поскольку это необратимая операция, ответом по умолчанию принято Нет. Щелкните Да, чтобы удалить объект.

Команда DSRM (рис. 5.5.) позволяет удалить объект компьютера из командной строки:

DSRM DN_объекта

Здесь *DN_объекта* — различающееся имя компьютера, например «CN=Desktop05, OU=Desktops, DC=povtas, DC=com».

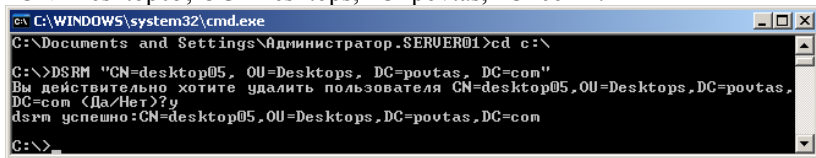


Рис. 5.5. Результат применения команды DSRM

Когда компьютер отсоединяется от домена (например, если администратор присоединяет его к другой рабочей группе или домену), он пытается удалить свою учетную запись из домена. Если это нельзя сделать (из-за отсутствия связи, проблем с сетью или недостаточных разрешений), учетная запись остается в Active Directory. Она сразу или со временем будет отображаться как отключенная. Если эта учетная запись больше не нужна, нужно удалить ее вручную.

Если компьютер не будет использоваться долгое время или его отключают от сети, его учетную запись можно отключить (рисунок 5-6). Такое действие отвечает принципу безопасности, по которому список участников безопасности разрешает проверку подлинности только минимальному числу учетных записей, необходимому для решения задач организации. Отключение учетной записи не изменяет SID компьютера или его членство в группах, поэтому, когда компьютер подключат к сети, его учетную запись можно снова включить.

Когда учетная запись отключена, компьютер не может установить с доменом безопасную связь. В результате пользователи, ранее не входившие в систему на этом компьютере и реквизиты которых не были на нем кэшированы, не смогут входить в систему, пока учетная

запись данного компьютера не будет включена и безопасный канал не будет восстановлен.

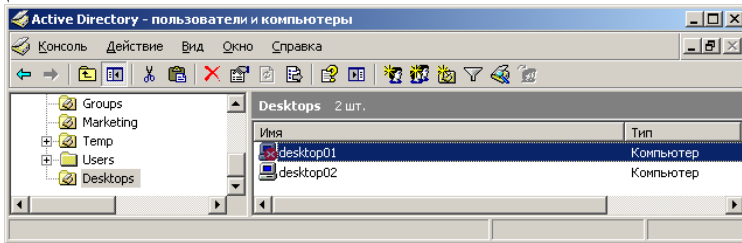


Рис. 5.6. Отключенная учетная запись компьютера

Для включения учетной записи компьютера нужно выделить компьютер и в меню Действие или в контекстном меню выбрать команду Включить учетную запись.

Отключать и включать компьютер из командной строки можно командой DSMOD, которая изменяет объекты Active Directory:

```
DSMOD COMPUTER DN_компьютера _DISABLED YES
```

```
DSMOD COMPUTER DN_компьютера _DISABLED NO
```

Если членство в группах и SID учетной записи компьютера, а также разрешения, назначенные этому SID, важны для функционирования домена, не следует удалять такую учетную запись. В этом случае может понадобиться переустановка учетной записи компьютера.

При переустановке учетной записи компьютера пароль на вход удаляется, но сохраняются все остальные свойства объекта. Без пароля данная учетная запись фактически становится «доступной» для использования. Любой компьютер теперь может присоединиться к домену по этой учетной записи.

На самом деле компьютер, который уже был присоединен к домену с этой учетной записью, тоже может использовать переустановленную запись, просто ему нужно повторно присоединиться к этому домену.

Команда Переустановить учетную запись доступна для выбранного объекта компьютера в меню Действие и в контекстном меню. Для переустановки учетной записи компьютера также можно применять команду DSMOD:

```
DSMOD computer DN_компьютера -reset
```

Команда NETDOM, входящая в средства поддержки Windows Server 2003, также позволяет переустановить учетную запись компьютера.

Выявление проблем с учетными записями компьютеров

Учетные записи компьютеров и безопасные отношения между компьютерами и их доменом работают весьма надежно. В редких случаях, когда учетная запись или безопасный канал перестают функционировать, признаки такой неполадки вполне очевидны. Наиболее типичные признаки проблем с учетными записями компьютеров следующие:

- сообщения при входе в систему о том, что связь с контроллером домена не может быть установлена, отсутствует учетная запись для данного компьютера или доверительные (то есть безопасные) отношения между компьютером и доменом были потеряны (см. пример на рис. 5.7.);
- сообщения об ошибках или записи в журнале событий о подобных проблемах или предположения об ошибке паролей, доверительных отношений, безопасных каналов или отношений с доменом или контроллером домена;
- отсутствие учетной записи компьютера в Active Directory.

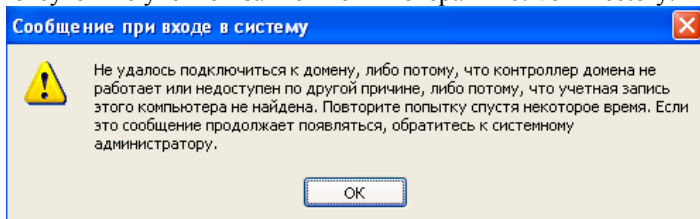


Рис. 5.7. Сообщение, выдаваемое клиентом Windows XP при входе в систему, о возможных проблемах с учетной записью компьютера

При устранении неполадок с учетными записями компьютеров следует придерживаться следующих правил.

1. Если данная учетная запись компьютера существует в Active Directory, ее нужно переустановить.
2. Если данной учетной записи компьютера нет в Active Directory, ее нужно создать.
3. Если компьютер еще принадлежит домену, его нужно удалить из домена, включив в какую-либо рабочую группу. Имя рабочей группы не имеет значения. Лучше всего методом проб найти имя, которое точно не используется.
4. Снова присоединить этот компьютер к домену; или присоединить другой компьютер, но его имя должно совпадать с именем данной учетной записи.

Для устранения любой неполадки с учетной записью компьютера используйте все четыре правила. Они могут применяться в произвольном порядке, за исключением правила 4, связанного с присоединением компьютера к домену, — эту операцию выполняйте в последнюю очередь.

Могут встречаться две ситуации.

В первой ситуации пользователь жалуется: при попытке входа в систему выдается сообщение, что учетная запись для данного компьютера, возможно, отсутствует. Применяя правило 1, вы открываете консоль *Active Directory* — *пользователи и компьютеры* и обнаруживаете, что данная учетная запись существует. Вы переустанавливаете учетную запись. Правило 2 не применяется — учетная запись существует. Затем, согласно правилу 3, вы отсоединяете данную систему от домена, после чего по правилу 4 снова присоединяете ее.

Во второй ситуации предположим, что учетная запись компьютера переустановлена случайно, тогда сначала применим правило 1. Хотя переустановка и случайна, необходимо продолжить восстановление согласно остальным трем правилам. Правило 2 не применяется, поскольку данная учетная запись существует в домене. Правило 3 говорит, что раз компьютер еще присоединен к домену, его нужно удалить из домена, а затем, по правилу 4, снова присоединить.

Анатомия объекта computer

В Active Directory представление компьютеров во многом подобно представлению пользователей: это объекты в составе каталога, для удобства администрирования объединенные в группы и подразделения. Равно как и объектам user, им предоставляются разрешения на доступ к ресурсам, к ним применяются групповые политики. Класс computer, к которому относятся эти объекты, наследует класс user, благодаря чему он в дополнение к нескольким собственным атрибутам включает все атрибуты данного класса.

Для того чтобы компьютеры могли входить в состав доменов, каждый из них должен иметь защищенный канал связи с контроллером домена. Такого рода канал представляет собой аутентифицируемое подключение, через которое можно передавать зашифрованные данные. Для его создания компьютер должен сообщить контроллеру домена свой пароль, который будет сверяться с паролем, хранящимся в учетной записи этого компьютера в Active Directory. Без такой учетной записи (представленной объектом computer) аутентификация компьютера просто невозможна.

По умолчанию объекты computer помещаются в контейнер cn=Computers, который находится в корневом каталоге домена. Однако при желании такие объекты можно создавать в любом месте дерева каталога в пределах домена. Более того, в Windows Server 2003 можно изменить задаваемое по умолчанию местоположение объектов computer. Список важнейших атрибутов объекта computer приведен в таблице 5.1.

Таблица 5.1. Атрибуты объекта computer

Атрибут	Описание
cn	Относительное отличительное имя объекта computer
dnsHostName	Полное DNS-имя компьютера
lastLogonTimestamp	Приблизительные значения даты и времени последнего подключения компьютера к домену. Этот атрибут был введен в Windows Server 2003
managedBy	Отличительное имя пользователя (или группы), отвечающего за управление данным компьютером
memberOf	Список отличительных имен групп, в которые входит данный компьютер
operatingSystem	Текстовое описание операционной системы, под управлением которой работает компьютер
operatingSystemHotFix	В настоящее время не используется
operatingSystemServicePack	Версия установленного на компьютере пакета обновлений
operatingSystemVersion	Версия операционной системы, под управлением которой работает компьютер
pwdLastSet	Большое целое число, представляющее время последней установки пароля данного компьютера
sAMAccountName	NetBIOS-имя компьютера.
userAccountControl	Набор битовых флагов, представляющих свойства учетной записи

6. Файлы и папки

Открытие общего доступа к папке

Открытие общего доступа к папке указывает *Службе доступа к файлам и принтерам сетей Microsoft* разрешить клиентам, на компьютерах которых запущена служба *Клиент для сетей Microsoft*, подключаться к этой папке и ее подпапкам. Для создания общей папки с помощью *Проводника Windows* нужно щелкнуть папку правой кнопкой, выбрать *Общий доступ и безопасность* и установить переключатель *Открыть общий доступ к этой папке* [1, 9, 10].

Вкладка *Доступ* окна свойств папки в *Проводнике Windows* доступна, только при локальном входе в систему или с помощью служб терминалов. Создать общую папку на удаленном компьютере нельзя. Для создания и управление общими папками можно использовать оснастку *Общие папки*.

В Windows Server 2003 уже настроено несколько стандартных административных общих ресурсов: системный каталог и корень каждого жесткого диска. Имя ресурса для них заканчивается знаком доллара (\$). Знаком доллара в конце сетевого имени обозначают скрытые общие папки. Они не видны в обозревателе, но к ним можно подключиться по UNC-имени вида \\имя_сервера\имя_общего_ресурса\$. К административным общим ресурсам могут подключаться только администраторы.

Для открытия общего доступа к папке, нужно подключиться к компьютеру из оснастки *Общие папки*. Выбрав компьютер, щелкните узел *Общие папки*, а затем в контекстном меню или в меню *Действие* выберите *Новый общий ресурс*. Мастер создания общих ресурсов содержит следующие страницы и настройки:

- *Путь к папке*. Указывается путь к общей папке на локальном жестком диске, например, если папка находится на диске D: сервера, путь к ней будет иметь вид D:\имя_папки.

- *Имя, описание и параметры*. Вводится имя общего ресурса. Имя ресурса вместе с именем сервера образуют UNC-имя вида \\имя_сервера\имя_общего_ресурса. чтобы сделать общий ресурс скрытым, нужно добавить знак доллара в конце сетевого имени. К скрытым общим папкам, созданным вручную, может подключиться любой пользователь, причем его права ограничиваются только разрешениями общего ресурса.

- *Разрешения*. Выбираются все подходящие разрешения для общего ресурса.

Управление общей папкой

Узел *Общие* в оснастке *Общие папки* содержит список всех общих ресурсов компьютера и для каждого из них предоставляет контекстное меню, которое позволяет прекратить доступ, открыть общий ресурс в *Проводнике* или настроить его свойства. Все свойства, которые предлагает заполнить *Мастер создания общих ресурсов*, можно изменить в окне свойств общего ресурса (рис. 6.1.).

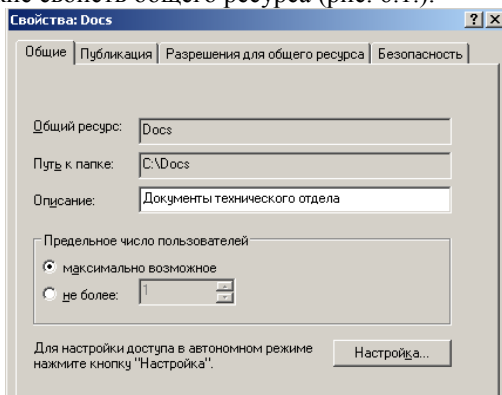


Рис. 6-1. Вкладка *Общие* диалогового окна свойств общей папки

Окно свойств общей папки содержит следующие вкладки:

- *Общие*. Указываются сетевое имя, путь к папке, описание, количество одновременных подключений пользователей и параметры работы с файлами в автономном режиме. Имя общего ресурса и путь к нему предназначены только для чтения. Чтобы переименовать общий ресурс, нужно сначала закрыть доступ, а затем создать общий ресурс с новым именем.
- *Публикация*. Если установить флажок *Опубликовать этот общий ресурс в Active Directory*, как показано на рис. 6.2., в Active Directory будет создан объект, представляющий эту общую папку.
- *Разрешения для общего ресурса*. Настраиваются разрешения доступа к общему ресурсу.
- *Безопасность*. Настраиваются разрешения NTFS для общей папки.

К свойствам объекта относятся описание и ключевые слова, по которым общую папку можно найти, используя диалоговое окно *Поиск: Пользователи, контакты и группы*. Если в раскрывающемся списке *Найти* выбрать значение *Общие папки*, это диалоговое окно трансформируется в окно *Поиск: Общие папки* (на рис. 6.3.).

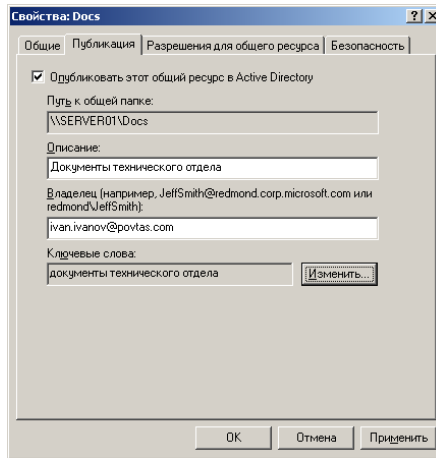
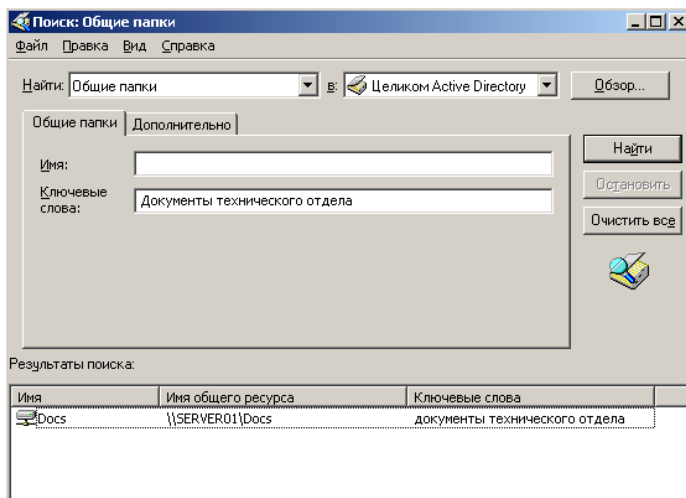
Рис. 6.2. Вкладка *Публикация* диалогового окна свойств общей папки

Рис. 6.3. Поиск общей папки

Настройка разрешений доступа к общему ресурсу

Доступные разрешения общего ресурса перечислены в таблице 6.1. Они позволяют настроить основные типы доступа к общей папке: *Чтение*, *Изменение* и *Полный доступ*.

Таблица 6.1. Разрешения для общего ресурса

Разрешение	Описание
Чтение	Можно просматривать имена папок, а также имена, содержимое и атрибуты файлов, запускать программы и обращаться к другим папкам внутри общей папки
Изменение	Можно создавать папки, добавлять файлы и редактировать их содержимое, изменять атрибуты файлов, удалять файлы и папки и выполнять действия, допустимые разрешением Чтение
Полный доступ	Можно изменять разрешения файлов, становится владельцами файлов и выполнять все действия, допустимые разрешением Изменение

Разрешения общего ресурса можно предоставлять или отменять. Действующим набором разрешений общего ресурса называют сумму разрешений, предоставленных пользователю и всем группам, членом которых он является. Например, если пользователь входит в группу с разрешением Чтение и в группу с разрешением Изменение, действующим разрешением считается Изменение. Тем не менее, запрет всегда приоритетнее разрешения. Например, если пользователь входит в группу с разрешением Чтение и в группу, которой запрещено разрешение Полный доступ, он не сможет прочесть файлы и папки внутри общего ресурса.

Разрешения общего ресурса определяют максимальные действующие разрешения для всех файлов и папок внутри общей папки. Назначая разрешения NTFS для отдельных файлов и папок, доступ можно ужесточить, но не расширить. Т.е., доступ пользователя к файлу или папке определяется наиболее жестким набором из разрешений общего ресурса и разрешений NTFS. Если разрешения NTFS дают группе полный доступ к папке, а разрешения общего ресурса остаются стандартными — группе Все предоставлено разрешение Чтение или даже Изменение — разрешения NTFS ограничиваются разрешением общего ресурса. Этот механизм означает, что разрешения общего ресурса усложняют управление доступом к ресурсам. Это одна из причин, по которой в организациях обычно назначают общим ресурсам открытые разрешения: группе Все дается разрешение Полный доступ, а для защиты папок и файлов используют только разрешения NTFS.

Управление сеансами пользователей и открытыми файлами

Для текущего обслуживания или настройки сервер иногда приходится переводить в автономный режим. В этом случае пользователи должны быть отключены от сервера, а файлы и папки закрыты. Поэтому целесообразно использовать оснастку *Общие папки*. Узел *Сеансы* оснастки *Общие папки* позволяет отследить количество пользователей, подключенных к определенному серверу и при необходимости отключить их. Узел *Открытые файлы* содержит список всех открытых файлов и блокировок файлов для одного сервера и позволяет отключить все открытые файлы. Перед выполнением этих операций нужно оповестить пользователя об отключении, чтобы он успел сохранить данные. Можно отправить текстовое сообщение, щелкнув правой кнопкой узел **Общие папки** и выбрав соответствующую команду. Сообщения пересылаются службой Messenger, которая использует имя компьютера, а не пользователя.

Настройка разрешений файловой системы

Серверы Windows поддерживают детализированный механизм управления доступом к файлам и папкам — разрешения NTFS. Разрешения доступа к ресурсам хранятся в виде *записей управления доступом* (access control entries, ACE) в таблице ACL, которая является частью дескриптора безопасности каждого ресурса. При обращении к ресурсу маркер безопасности доступа пользователя, содержащий *идентификаторы защиты* (security identifier, SID) учетной записи пользователя и групп, членом которых тот является, сравнивается с идентификаторами SID в ACE-записях таблицы ACL.

Для настройки безопасности файлов и папок на любом томе NTFS нужно щелкнуть ресурс правой кнопкой, в контекстном меню выбрать *Свойства* или *Общий доступ и безопасность* и перейти на вкладку *Безопасность*. Пример вкладки *Безопасность* окна свойств папки Docs см. на рис. 6.4.

Редактор ACL состоит из трех диалоговых окон.

Первое диалоговое дает общую картину настроек безопасности и разрешений для ресурса и позволяет выбрать отдельную учетную запись, для которой определен доступ, чтобы просмотреть шаблоны разрешений, назначенные этому пользователю, группе или компьютеру. Каждый шаблон в этом окне — совокупность разрешений, которые вместе обеспечивают некий типичный уровень доступа.

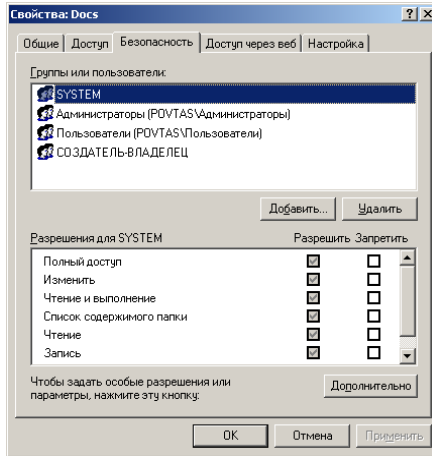
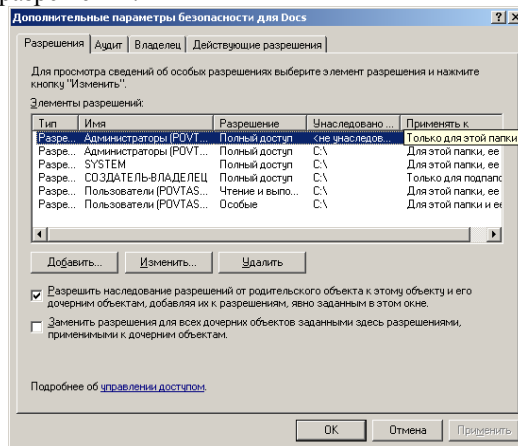


Рис. 6.4. Редактор ACL в окне свойств папки Docs

Чтобы более подробно просмотреть таблицу ACL, щелкните кнопку *Дополнительно*, откроется второе окно редактора ACL — *Дополнительные параметры безопасности для Docs*, показанное на рис. 6.5. Здесь перечислены конкретные записи управления доступом, назначенные данному файлу или папке. Сведения в этом перечне максимально приближены к реальной информации, которая хранится в самой таблице ACL. Второе диалоговое окно позволяет также настраивать аудит, управлять правами владения и определять действующие разрешения.

Рис. 6.5. Диалоговое окно *Дополнительные параметры безопасности редактора ACL*

Если выбрать разрешение в списке *Элементы разрешений* и щелкнуть *Изменить*, откроется третье диалоговое окно редактора ACL. В окне *Элемент разрешения для Docs*, показанном на рис. 6.6, перечислены подробные, наиболее детализированные разрешения, которые составляют элемент разрешений в списке *Элементы разрешений* во втором диалоговом окне и в списке *Разрешения для* в первом окне.

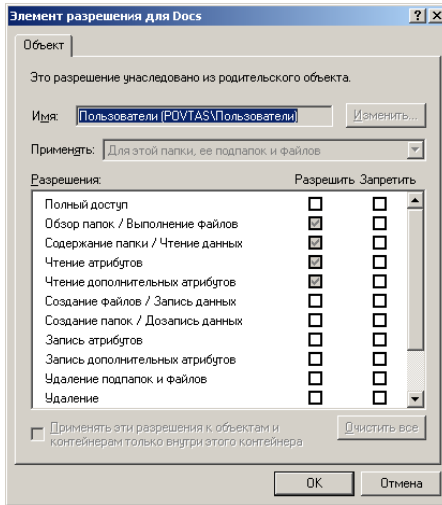


Рис. 6.6. Диалоговое окно *Элемент разрешения* редактора ACL

Любому участнику безопасности можно предоставить или запретить доступ к ресурсу. В Windows Server 2003 допустимые участники безопасности: пользователи, группы, компьютеры и специальный класс объектов InetOrgPerson, который представляет пользователей в некоторых ситуациях при совместной работе разных платформ.

Чтобы добавить разрешение, щелкните *Добавить* в первом или втором диалоговом окне редактора ACL. В диалоговом окне *Выбор: «Пользователи», «Компьютеры» или «Группы»* выберите нужного участника безопасности и разрешения. Для удаления явного разрешения, которое вы добавили в ACL, выберите нужный пункт списка и щелкните *Удалить*.

Для изменения разрешения нужно на вкладке *Безопасность* окна свойств установить или снять флажки *Разрешить* или *Запретить*, в результате чего применится соответствующий шаблон разрешений. Для более тонкой настройки щелкните кнопку *Дополнительно*,

выберите элемент разрешения и щелкните кнопку *Изменить*. Изменить можно только явные разрешения.

Windows Server 2003 позволяет добавлять компьютеры или группы компьютеров в ACL, обеспечивая этим большую гибкость управления доступом к ресурсам на основе клиентских компьютеров, независимо от пользователя, который пытается получить доступ. Например, в комнате отдыха сотрудников установлен компьютер с общим доступом, но руководители не должны просматривать с него секретные данные. Если добавить этот компьютер в таблицы ACL и запретить с него доступ к секретным данным, руководитель не сможет обратиться к секретным данным из комнаты отдыха и будет работать с ними только с собственного компьютера.

Windows Server 2003 также позволяет управлять доступом к ресурсу в зависимости от способа входа в систему. Можно добавить в ACL особые учетные записи: *Интерактивные* — пользователи, которые зарегистрировались локально, *Сеть* — сетевое подключение, например система Windows, на которой запущена служба *Клиент для сетей Microsoft*, и *Пользователь сервера терминалов* — пользователи, подключившиеся через службу *Дистанционное управление рабочим столом* или службы терминалов.

Шаблоны разрешений на вкладке *Безопасность* первого диалогового окна представляют собой совокупность особых разрешений, которые полностью перечислены в третьем диалоговом окне *Элемент разрешения*. Рассмотрим наиболее значимые из них.

- *Чтение и выполнение*. Чтобы позволить пользователям открывать и читать файлы и папки, нужно назначить им этот шаблон разрешений. Он также позволяет пользователю скопировать ресурс, если тот имеет разрешение на запись для целевой папки или носителя. В Windows нет разрешений, запрещающих копирование.

- *Запись и Изменение*. Шаблон *Запись* позволяет создавать новые файлы и папки и изменять содержимое и атрибуты файлов и дополнительные атрибуты, определяемые приложением, которое отвечает за этот документ. Шаблон *Изменение* дополнительно разрешает удалить объект.

- *Смена разрешений*.. Изменять разрешения может владелец ресурса. Кроме того, это может сделать любой пользователь с действующим разрешением *Смена разрешений*, которое задают с помощью третьего диалогового окна *Элемент разрешения для Docs* редактора ACL.

Наследование

Windows Server 2003 поддерживает наследование разрешений, которое означает, что по умолчанию разрешения папки распространяются на все ее файлы и подпапки. Любые изменения родительской таблицы ACL будут отражаться на всем содержимом папки. Наследование позволяет управлять ветвями ресурсов в единых точках администрирования с помощью одной таблицы ACL.

Наследование работает благодаря двум характеристикам дескриптора безопасности ресурса. В первую очередь, по умолчанию разрешения наследуются. Разрешение *Чтение и выполнение* (Read & Execute) на рис. 6-5 распространяется на саму папку, подпапки и файлы. Тем не менее, одного этого недостаточно, чтобы наследование работало. Во-вторых, по умолчанию при создании новых объектов установлен флажок *Разрешить наследование разрешений от родительского объекта к этому объекту...*, видимый на том же рисунке. Таким образом, созданный файл или папка будут наследовать разрешения у своего родителя, а изменения разрешений родителя будут отражаться на дочерних файлах и папках. Важно понять такую двухэтапную реализацию разрешений, поскольку она дает нам два способа управления наследованием: со стороны родительского и дочернего объектов.

Унаследованные разрешения по-разному отображаются в каждом окне редактора ACL. В первом и третьем диалоговых окнах [на вкладке *Безопасность* и в окне *Элемент разрешения*] унаследованные разрешения отображаются в виде «серых» флажков, чтобы отличать их от явных разрешений, то есть назначенных ресурсу напрямую. Второе диалоговое окно — *Дополнительные параметры безопасности* — содержит папки, от которых наследуется каждый элемент разрешения.

Наследование позволяет настраивать разрешения на вершине дерева папок. Эти разрешения и их изменения будут распространяться на все файлы и папки в дереве, для которых по умолчанию разрешено наследование. Впрочем, иногда требуется изменить разрешения подпапки или файла, чтобы расширить или ограничить доступ пользователя или группы. Унаследованные разрешения нельзя удалить из ACL. Их можно перекрыть, назначив явные разрешения. Либо можно отменить наследование и создать ACL, содержащую только явные разрешения. Для замены унаследованных разрешений явными следует установить соответствующий флажок.

Чтобы отменить все унаследованные разрешения, откройте диалоговое окно *Дополнительные параметры безопасности ресурса* и снимите флажок *Разрешить наследование разрешений от*

родительского объекта к этому объекту.... Все разрешения, унаследованные от родительского объекта, будут заблокированы. После нужно назначить явные разрешения, чтобы проконтролировать доступ к ресурсу.

Windows помогает задать явные разрешения, когда наследование отменяется. Появится окно (рис. 6.7) с вопросом, как поступить с разрешениями: *Копировать* или *Удалить*.

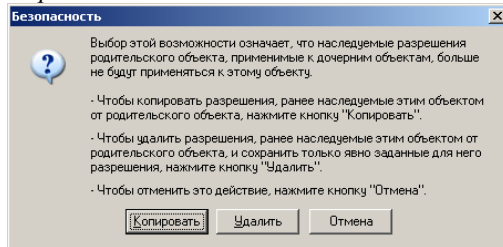


Рис. 6.7. Копирование или удаление элементов разрешений

По щелчку *Копировать* создаются явные разрешения, идентичные унаследованным. Затем можно удалить отдельные элементы разрешений, которые не должны влиять на ресурс. Если же выбрать *Удалить*, предлагается пустая таблица ACL, которую следует заполнить элементами разрешений. Результат одинаков в обоих случаях: таблица ACL заполнена явными разрешениями. Если новая ACL сильно отличается от унаследованной, лучше удалить наследуемые разрешения, если незначительно - копировать разрешения. Снимая флажок *Разрешить наследование разрешений от родительского объекта к этому объекту...*, полностью блокируется наследование. Доступ к ресурсу регулируется только явными разрешениями, назначенными для файла или папки. Любые изменения ACL родительской папки не будут влиять на ресурс; даже если родительские разрешения являются наследуемыми, дочерний ресурс не наследует их.

Наследование можно восстановить двумя способами: со стороны дочернего ресурса или со стороны родительской папки. Результаты немного различаются. Восстановить наследование для ресурса может понадобиться, если вы случайно отменили его или изменились требования организации. Нужно установить флажок *Разрешить наследование разрешений...* в диалоговом окне *Дополнительные параметры безопасности*. Наследуемые разрешения родительской папки будут распространяться на дочерний ресурс. Однако останутся все явные разрешения, назначенные ресурсу. Итоговая ACL будет

содержать совокупность явных разрешений, которые можно удалить, и унаследованных разрешений. По этой причине не будет видно некоторых унаследованных разрешений в первом и третьем диалоговых окнах редактора ACL. Например, если группе Sales Reps явно назначено разрешение *Чтение и выполнение* в отношении какого-нибудь ресурса, которое назначено и родительской папке, то при восстановлении наследования со стороны дочернего ресурса, ему назначаются и унаследованные, и явные разрешения.

Второй метод восстановления наследования — со стороны родительской папки.

В диалоговом окне *Дополнительные параметры безопасности* для родительской папки нужно установить флажок *Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам*. В результате все ACL подпапок и файлов будут удалены. На дочерние ресурсы распространяются разрешения родительской папки. Это можно представить как сквозное применение разрешений родителя. После выбора этого варианта любые явные разрешения, назначенные подпапкам и файлам, удаляются. Наследование восстанавливается, поэтому любые изменения ACL родительской папки отражаются на подпапках и файлах. В этот момент подпапкам и файлам можно назначить новые явные разрешения. Флажок *Заменить разрешения...* выполняет свою функцию, только когда его отмечают, однако в дальнейшем разрешения родительской папки не будут заменять собой явные разрешения.

Действующие разрешения

Часто пользователи принадлежат к нескольким группам с разными уровнями доступа к ресурсам. Когда ACL содержит несколько элементов, нужно уметь определять разрешения пользователя, исходя из разрешений групп, членом которых он является. Конечные разрешения называют *действующими*.

Существует несколько правил, по которым определяются действующие разрешения:

1. Разрешения файлов приоритетнее разрешений папок;
2. Разрешения, позволяющие доступ, суммируются;
3. Разрешения, запрещающие доступ, приоритетнее позволяющих;
4. Явные разрешения приоритетнее унаследованных.

Для того, чтобы узнать действительные права доступа пользователя имеется вкладка *Действующие разрешения* диалогового

окна *Дополнительные параметры безопасности*, которая дает довольно точное приближение итоговых разрешений доступа пользователя к ресурсу (рис. 6.8).

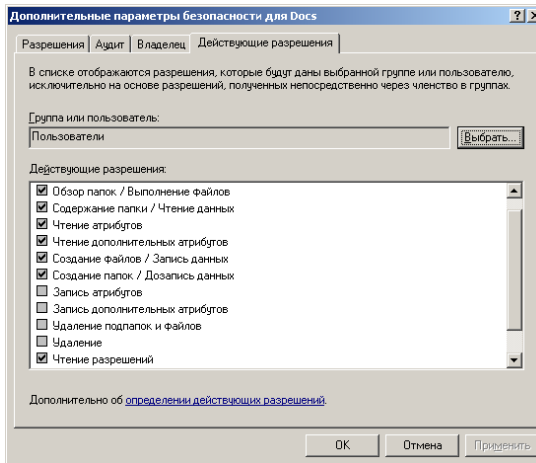


Рис. 6.8. Вкладка *Действующие разрешения* диалогового окна *Дополнительные параметры безопасности*

Щелкните кнопку *Выбрать* и укажите группу или пользователя, которых нужно проанализировать. Операционная система построит приближенный список действующих разрешений. В нем не учтены ни разрешения общего ресурса, ни принадлежность учетной записи особым группам.

Кроме того, ACL может содержать элементы, которые могли бы обеспечивать пользователям различный уровень доступа в зависимости от способа входа в систему — локально или удаленно. Также можно определить действующие разрешения для встроенных или особых учетных записей, таких как *Интерактивные* и *Сеть*.

Права владения ресурсом

ОС Windows Server 2003 поддерживает специального участника безопасности — *Создатель-владелец*. Помимо этого, в дескрипторе безопасности ресурса есть запись, определяющая владельца объекта.

Когда пользователь создает файл или папку, он становится создателем и первым владельцем этого ресурса. Любые разрешения, предоставленные учетной записи *Создатель-владелец* для родительской папки, явно назначаются пользователю в отношении этого нового ресурса. Если для этой папки пользователям

предоставлены разрешения *Создание файлов/Запись данных* и *Чтение и выполнение*, а учетной записи *Создатель-владелец* — разрешение *Полный доступ*, то такой набор разрешений позволил бы пользователю Мария создать файл. Как создатель файла, Мария имела бы к нему полный доступ. Пользователь Людмила также могла бы создать файл и получить к нему полный доступ. Однако Людмила и Мария могли бы лишь читать файлы друг друга. При этом Людмила могла бы изменить ACL своего файла. Разрешение *Полный доступ* включает разрешение *Смена разрешений*.

Если бы Людмила изменила ACL своего файла и запретила себе полный доступ, она по-прежнему смогла бы изменять ACL этого файла, т.к. владелец объекта всегда имеет такое право. Поэтому пользователи не могут навсегда заблокировать собственные файлы и папки.

Следует управлять правами владения так, чтобы объектом всегда владел соответствующий пользователь. Это нужно из-за того, что пользователи могут изменять ACL собственных объектов. Кроме того, такие технологии, как квотирование диска, полагаются на атрибут владения при подсчете места на диске, занятого некоторым пользователем. Владелец указывается в дескрипторе безопасности объекта. Первоначальным владельцем становится создатель файла или каталога. Право владения можно принимать или передавать следующим образом:

1. Администраторы могут становиться владельцами.

Пользователь из группы *Администраторы* или обладающий правом *Смена владельца* может получить во владение любой объект в системе. Для этого нужно перейти на вкладку *Owner* в диалоговом окне *Дополнительные параметры безопасности*, показанном на рис. 6.9, выбрать в списке свою учетную запись пользователя и щелкнуть *Применить*. Чтобы стать владельцем всех подпапок и файлов нужно установить флажок *Заменить владельца подконтейнеров и объектов*.

2. Права владения могут изменять пользователи с разрешением *Смена владельца*. Разрешение *Смена владельца* может быть предоставлено любому пользователю или группе, и они смогут завладеть ресурсом и изменить ACL, чтобы получить достаточные разрешения.

3. Администраторы могут передавать права владения. Администратор может завладеть любым файлом или папкой. Далее он может изменить разрешения доступа к ресурсу и предоставить разрешение *Смена владельца* другому пользователю, который, в свою очередь, может завладеть этим ресурсом.

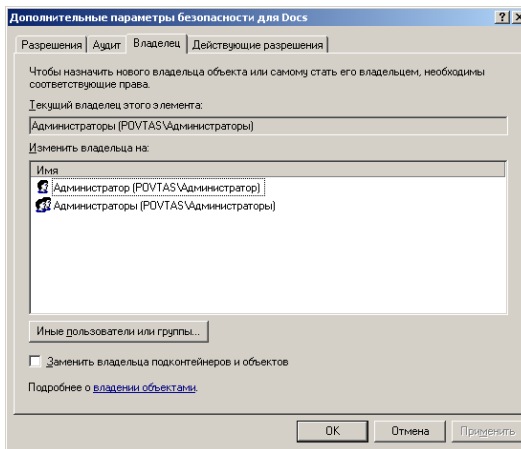


Рис. 6.9. Вкладка *Владелец* диалогового окна *Дополнительные параметры безопасности*

4. Пользователи с привилегиями *Восстановление файлов и каталогов*. Пользователь с такими полномочиями может передать права владения файлом другому пользователю. Если дана привилегия *Восстановление файлов и каталогов*, нужно щелкнуть кнопку *Иные пользователи или группы* и выбрать нового владельца.

Аудит доступа к файловой системе

Как правило, аудит доступа к файловой системе используется для оценки использования ресурсов и определения потенциально слабых мест в системе защиты. ОС Windows Server 2003 поддерживает подробный аудит на основе учетных записей пользователей или групп и определенных действий этих записей. Для настройки аудита необходимо указать его параметры, включить политику и изучить события в журнале безопасности.

Чтобы указать действия, которые нужно контролировать, следует настроить параметры аудита в диалоговом окне *Дополнительные параметры безопасности* объекта (рис. 6.10) .

Чтобы выбрать объект для аудита следует щелкнуть кнопку *Добавить*. Далее в диалоговом окне *Элемент аудита* нужно указать разрешения, которые нужно отслеживать (рис. 6.11). Аудиту подлежат успешные и неудачные попытки доступа учетной записи к ресурсу с использованием каждого из назначенных объекту разрешений.

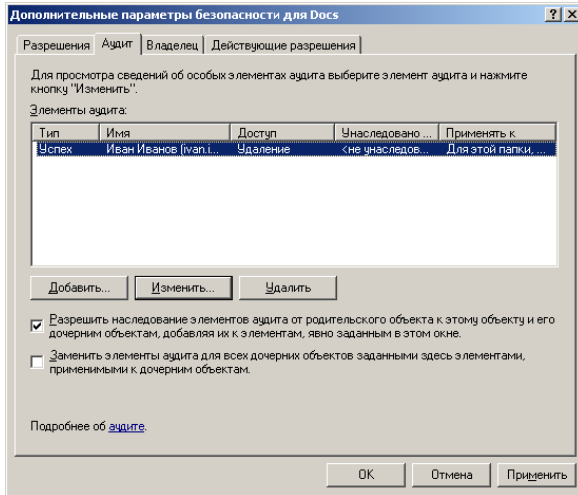


Рис. 6.10. Вкладка *Аудит* диалогового окна *Дополнительные параметры безопасности*

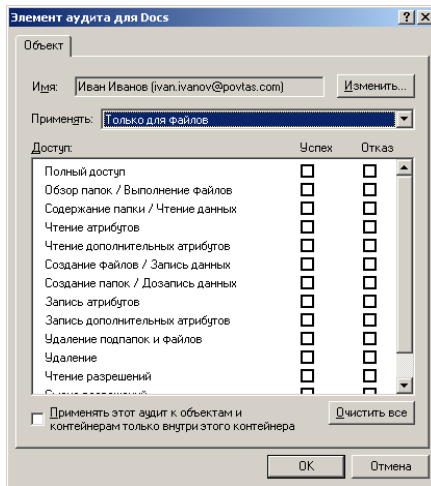


Рис. 6.11. Диалоговое окно *Элемент аудита*

Аудит успешных попыток доступа обычно используют для следующих целей:

- регистрация попыток доступа к ресурсам для составления отчетов и выписки счетов;

- мониторинг попыток доступа, которые бы указали, что пользователи выполняют непредусмотренные действия, то есть разрешения настроены недостаточно жестко;

- выявление попыток доступа, которые нехарактерны для данной учетной записи; это может быть признаком того, что учетная запись взломана.

Аудит неудачных попыток служит для:

- обнаружения попыток доступа к секретному ресурсу;
- определения неудачных попыток обращения к файлу или папке, доступ к которой действительно требуется пользователю.

Параметры аудита удовлетворяют правилам наследования. Наследуемые параметры аудита распространяются на объекты, разрешающие наследование.

Журналы аудита очень быстро растут, поэтому следует следить за минимальным количеством событий, которых достаточно для решения задачи. Если настроить аудит успешных и неудачных попыток доступа к часто используемой папке для группы *Все* и контролировать все виды доступа, будут созданы огромные журналы аудита, которые могут снизить производительность сервера и крайне затруднить поиск нужных событий.

Аудит необходимо включить через политику безопасности. После включения аудита подсистема безопасности начинает принимать во внимание параметры аудита и регистрировать соответствующие попытки доступа.

Политику аудита можно включить на изолированном сервере в консоли *Локальная политика безопасности* и на контроллере домена в консоли *Политика безопасности контроллера домена*. Раскройте узел *Локальные политики*, затем *Политика аудита* и дважды щелкните политику *Аудит доступа к объектам*. Выберите *Определить следующие параметры политики* и укажите, какие попытки доступа должны подлежать аудиту.

Аудит можно включить на одном или нескольких компьютерах, используя объекты групповой политики (ОГП) Active Directory. Узел *Политика аудита* расположен в дереве *Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Политика аудита*. Как и остальные групповые политики, политика аудита влияет на все компьютеры, расположенные в области ее действия.

После того, как элементы аудита файлов и папок настроены и аудит доступа к объектам включен через локальную или групповую политику, система начинает регистрировать попытки доступа согласно

элементам аудита. Можно просмотреть и изучить результаты аудита в журнале безопасности с помощью оснастки *Просмотр событий*, показанной на рис. 6.12. Размер журнала безопасности зависит от типа событий, подлежащих аудиту. Можно отсортировать собранные данные, чтобы быстрее найти события доступа к объекту.

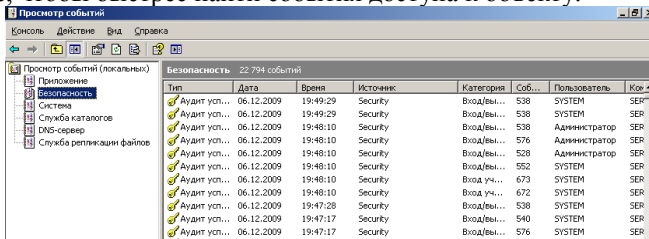


Рис. 6.12. Журнал безопасности в оснастке *Просмотр событий*

Кроме того, можно отфильтровать журнал событий. Для этого в меню **Вид** следует выбрать **Фильтр** или щелкнуть узел журнала безопасности и в контекстном меню или в меню **Действие** выбрать **Свойства**, после чего перейти на вкладку **Фильтр**. Она позволяет указать условия поиска, включая тип событий, источник события, категорию, пользователя, компьютер и временной диапазон (рис. 6.13).

Также, можно экспортировать журнал безопасности. Для этого в контекстном меню журнала нужно выбрать **Сохранить файл журнала как...** Файлы собственных журналов Windows имеют разрешение .evt. Их можно открыть на другом компьютере с помощью оснастки *Просмотр событий*. Либо можно сохранить журнал в текстовом файле в формате с разделителями (запятыми или символами табуляции).

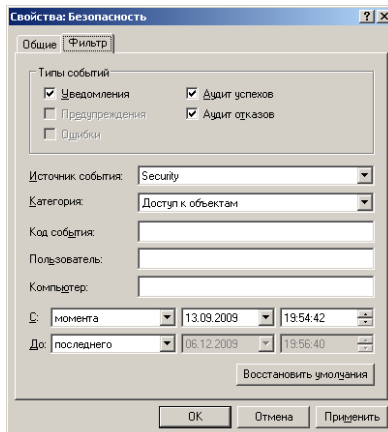


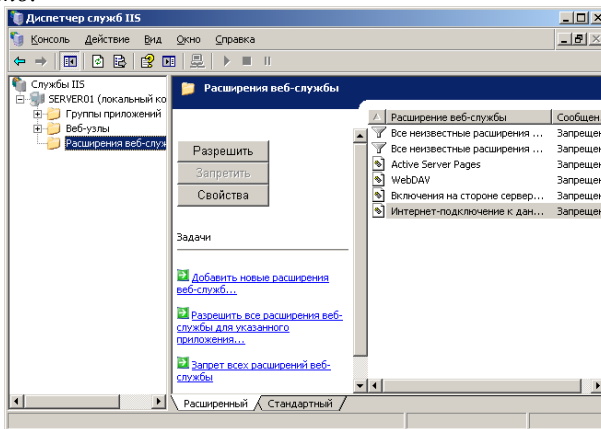
Рис. 6.13. Вкладка *Фильтр*

Администрирование служб IIS

Общий доступ к файлам и папкам можно организовать с помощью служб FTP и Web (HTTP). Для снижения риска атаки на системы Windows Server 2003 служба IIS по умолчанию не устанавливается. Ее нужно добавить с помощью мастера *Установка компонентов Windows* из приложения *Установка и удаление программ* в *Панели управления*.

При установке IIS создается стандартный Web-узел, позволяющий легко и быстро реализовать Web-среду, которую затем можно изменить. Windows Server 2003 содержит средства управления службой IIS и ее узлами [1, 8].

По умолчанию службы IIS настроены на работу только со статическим содержимым. Чтобы активировать динамическое содержимое, выберите узел *Расширения веб-службы* консоли *Диспетчер служб IIS*. Изначально все расширения отключены (рис. 6.14). Далее выберите нужное расширение и щелкните кнопку *Разрешить*.

Рис. 6.14. Консоль *Диспетчер служб IIS*

При обращении клиента к ресурсу IIS происходят следующие процессы.

1. Клиент вводит URL в одной из следующих форм:

`http://dns_имя_домена/виртуальный_каталог/страница.htm`
или

`ftp://dns_имя_домена/виртуальный_каталог`

2. Служба DNS преобразует введенное имя в IP-адрес и возвращает его клиенту.

3. Клиент подключается к серверу, используя полученный адрес и порт (обычно с номером 80 для HTTP и с номером 21 для FTP).

4. URL содержит не физический путь к ресурсу на сервере, а его виртуализацию. Сервер преобразует входящий запрос в физический путь и передает соответствующие ресурсы клиенту.

5. Этот процесс можно защитить с помощью механизмов проверки подлинности (заставив пользователей предоставлять имя и пароль) и авторизации (управляя доступом посредством разрешений).

При установке IIS настраивается единственный Web-узел — *Веб-узел по умолчанию*. Чтобы обратиться к этому Web-узлу, нужно открыть обозреватель и ввести `http://server01.povtas.com`. Будет отображена страница *В процессе разработки*.

Запрос браузера к Web-серверу направляется по IP-адресу сервера, который зарегистрирован в DNS для указанного URL. URL включается в запрос и часто содержит только имя узла (например, `www.bstu.ru`).

На вкладке *Веб-узел* в окне свойств Web-узла по умолчанию (см. рис. 6.15), видно, что для данного узла в списке выбора IP-адреса указано *Значения не присвоены* и задан порт 80. Запрос достигает порта 80 на сервере, который определяет, что запрос обращен к узлу *Веб-узел по умолчанию*. Если URL содержит только имя узла (например, `www.microsoft.com` или `server01.povtas.com`), то нужная страница извлекается из домашнего каталога. Вкладка *Домашний каталог*, показанная на рис. 6.16, указывает физический путь к домашнему каталогу (обычно `C:\inetpub\wwwroot`).

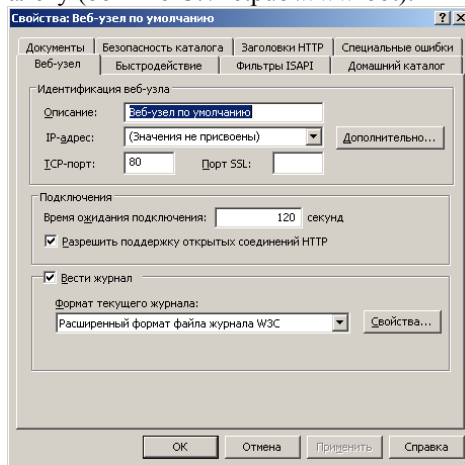


Рис. 6.15. Вкладка Веб-узел диалогового окна свойств Web-узла по умолчанию

Какой именно файл следует вернуть клиенту определяется на вкладке **Документы**, показанной на рис. 6.17. Служба IIS ищет файлы в указанном порядке. Как только файл с указанным именем по локальному пути к домашнему каталогу найден, запрошенная страница возвращается клиенту и сервер прекращает поиск остальных соответствий. Если страницу не удастся найти, IIS возвращает клиенту ошибку 404 — *Файл не найден*.

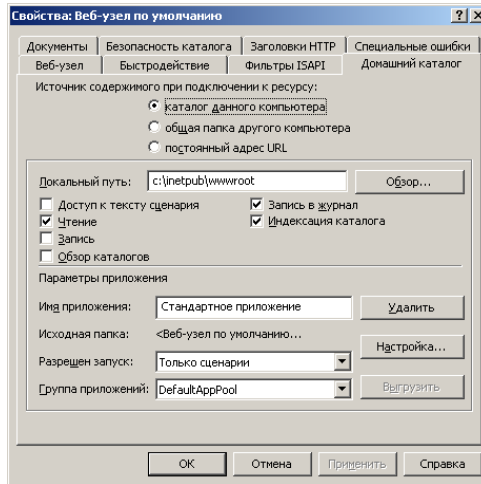
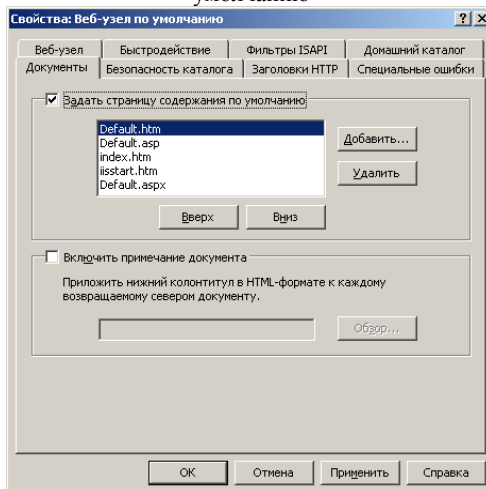
Рис. 6.16. Вкладка *Домашний каталог* диалогового окна свойств Web-узла по умолчанию

Рис. 6.17. Вкладка *Документы* диалогового окна свойств Web-узла

Чтобы создать Web-узел, нужно открыть консоль IIS Manager, щелкнуть узел *Веб-узлы* или существующий Web-узел правой кнопкой и выбрать *Создать Веб-узел*. Чтобы настроить Web-узел, откройте окно его свойств. Можно настроить IP-адрес данного узла. Если серверу назначено несколько IP-адресов, каждый из них может представлять отдельный Web-узел. Несколько узлов можно также разместить, используя несколько портов или заголовков узла. Кроме того, можно настроить путь к домашнему каталогу, а также изменить список или порядок документов, которые возвращаются в качестве стандартной страницы.

URL может содержать более сложную информацию о пути, например `http://www.bstu.ru/server2003`. Этот URL не запрашивает конкретную страницу, поскольку в конце адреса нет расширения `.htm` или `.asp`. Вместо этого он запрашивает информацию из каталога `server2003`. Сервер воспринимает эту дополнительную часть URL как виртуальный каталог. Папка, содержащая файлы, на которую ссылаются по имени `server2003`, может находиться где угодно, в том числе и на другом сервере. Чтобы создать виртуальный каталог, щелкните Web-узел правой кнопкой и выберите *Создать Виртуальный каталог*. Мастер предложит ввести псевдоним, который можно будет указывать как папку в URL, и физический путь к соответствующему ресурсу на локальном томе или на удаленном сервере.

Виртуальный Web-каталог на диске NTFS можно создать в окне свойств папки, настроив соответствующие параметры на вкладке *Доступ через веб*. FTP-узлы работают и управляются аналогично Web-узлам. IIS устанавливает один FTP-узел — *FTP-узел по умолчанию* — и настраивает его, чтобы тот отвечал на все входящие FTP-запросы, поступающие на порт 21. FTP-узел возвращает клиенту список файлов в папке, указанной на вкладке *Домашний каталог*. FTP-узлы также могут содержать виртуальные каталоги, например, запросы по адресам `ftp://server01.povtas.com/pub` и `ftp://server01.povtas.com/vendor_uploads` могут возвращать ресурсы с разных серверов. Служба FTP не поддерживает документы по умолчанию.

Мощные IIS серверы могут содержать десятки тысяч узлов, каждый со своими особыми параметрами. Потеря всей этой конфигурационной информации может быть болезненной: обычное архивирование файловой системы при сбое позволит восстановить файлы данных, но конфигурация будет утеряна. Для защиты

конфигурации IIS необходимо заархивировать или восстановить метабазу — XML-документ, в котором хранятся параметры конфигурации. Щелкните узел сервера в IIS Manager правой кнопкой и выберите *Все задачи\Архивирование и восстановление конфигурации*.

Защиту файлов, к которым обращаются через IIS, можно разделить на несколько категорий: проверка подлинности, авторизация через NTFS-разрешения и IIS-разрешения. Проверка подлинности — это процесс анализа реквизитов, предоставленных в форме имени пользователя и пароля. По умолчанию все запросы к IIS выполняются от имени пользователя с учетной записью IUSR-имя-компьютера. Прежде чем ограничивать доступ пользователей к ресурсам, необходимо создать локальные или доменные учетные записи и настроить проверку более высокого уровня, чем стандартная анонимная проверка подлинности.

Методы проверки подлинности можно настроить на вкладке *Безопасность каталога* в окне свойств сервера, Web- или FTP-узла, виртуального каталога или файла.

Существуют следующие варианты проверки подлинности средствами Web.

- Анонимная проверка подлинности. Пользователи, не указывая имя пользователя и пароль, могут получить доступ к открытой области Web-узла.
- Обычная проверка подлинности. У пользователя должна быть локальная или доменная учетная запись. Реквизиты передаются открытым текстом.
- Краткая проверка подлинности. Аналог обычной проверки с дополнительной защитой передаваемых по сети реквизитов пользователя.
- Расширенная краткая проверка подлинности. Работает, когда учетная запись пользователя хранится в Active Directory. Подразумевает получение и хранение реквизитов пользователей на контроллере домена.
- Встроенная проверка подлинности Windows. Получает информацию посредством безопасной формы проверки подлинности, при которой имя пользователя и пароль хэшируются перед передачей по сети.
- Проверка подлинности по сертификату. Добавляет защиту SSL (Secure Sockets Layer), благодаря использованию сертификатов сервера, клиента или обеих сторон.
- Проверка подлинности в системе .NET Passport. Предоставляет единую службу входа через SSL, перенаправление HTTP, файлы

cookies, Microsoft JScript и стойкое шифрование симметричным ключом.

Кроме вышеперечисленных, имеются некоторые варианты проверки подлинности средствами FTP.

- Анонимная проверка подлинности. Пользователи могут получить доступ к открытой области FTP-узла, не указывая имя пользователя и пароль.

- Обычная проверка подлинности. Требуется, чтобы пользователь ввел имя и пароль, которые соответствуют действительной учетной записи Windows.

Когда проверка подлинности настроена, назначают разрешения доступа к файлам и папкам. Разрешения NTFS — наиболее распространенный способ управления доступом к ресурсам через IIS. Поскольку разрешения NTFS назначают файлу или папке, они действуют независимо от способа доступа к ресурсу. IIS также назначает разрешения узлам и виртуальным каталогам. Разрешения безопасности каталога, назначенные узлу или виртуальному каталогу, распространяются на всех пользователей и группы.

В таблице 6.2 подробно описаны уровни Web-разрешений.

Таблица 6.2. Разрешения каталогов IIS

Разрешение	Описание
Чтение, используется по умолчанию	Пользователи могут просматривать содержимое и свойства файлов
Запись	Пользователи могут изменять содержимое и свойства файлов
Доступ к тексту сценария	Пользователи могут получить доступ к исходному коду файлов. Этот вариант доступен только при наличии разрешений Чтение или Запись. Пользователи получают доступ к исходному коду файлов. Если назначено разрешение Чтение, исходный код можно читать. Если назначено разрешение Запись, исходный код можно изменять.
Обзор каталогов	Пользователи могут просматривать списки и коллекции файлов

Разрешения Выполнение (Execute) регулируют уровень безопасности выполнения сценариев (таблица 6.3).

Таблица 6.3. Разрешения на выполнение приложений

Разрешение	Описание
Нет	Запрещает запуск любых приложений или сценариев
Только сценарии	Позволяет приложению, связанному с ядром сценариев, выполняться в этом каталоге без наличия разрешений, назначенных исполняемым программам.
Сценарии и исполняемые файлы	Позволяет любому приложению выполняться в этом каталоге, включая приложения, связанные с ядром сценариев, и двоичные программы Windows (файлы dll и exe).

При одновременном использовании разрешений IIS и NTFS, действуют наиболее жесткие из них.

7. Архивация и восстановление данных

Введение в архивацию

Архивация - это процесс выполнения сжатия данных с целью уменьшения объема пространства занимаемого данными, хранящимися на дисках сервера. В состав Windows Server 2003 входит программа архивации Ntbackup. Она обеспечивает большинство функций, которые встречаются в средствах сторонних разработчиков, включая возможность составления расписания архивации и взаимодействия со *Службой теневого копирования тома* (Volume Shadow Copy Service, VSS) и системой RSM (Removable Storage Management) [1, 5, 9].

Запустить программу резервного копирования можно двумя способами:

1. В меню *Пуск* следует выбрать *Все программы\Стандартные\Служебные\Архивация данных*.
2. Из диалогового окна *Запуск программы* командой *ntbackup.exe*.

В первый раз утилита резервного копирования запускается в режиме мастера (см. рис. 7.1).

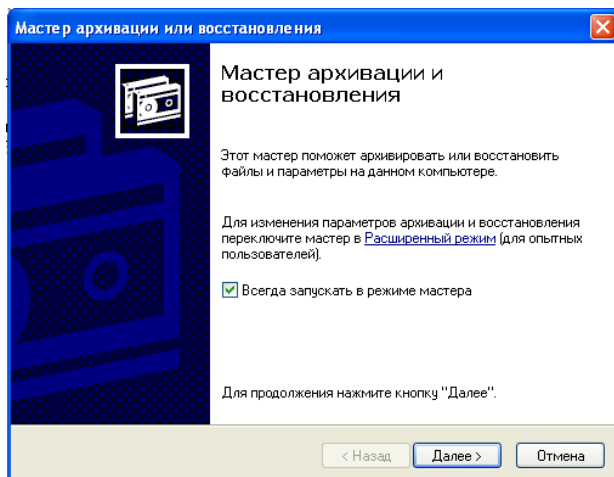


Рис. 7.1. Окно *Мастера архивации или восстановления*

Резервное копирование можно выполнить либо вручную, на вкладке *Архивация*, либо с помощью мастера (рис. 7.2). Кроме того,

можно составить расписание для автоматического выполнения заданий архивации. Программа Backup позволяет также восстанавливать данные вручную, на вкладке *Восстановление и управление носителем*, или с помощью мастера *Мастер восстановления*.

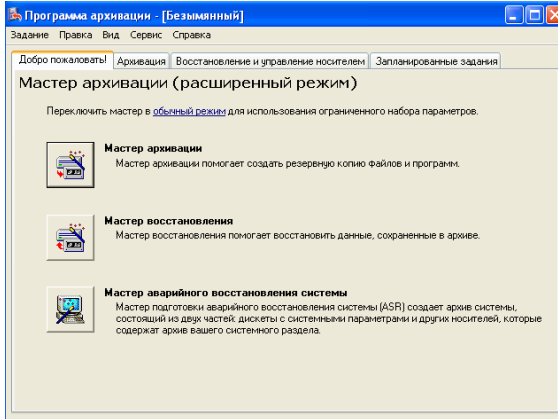


Рис. 7.2. Вкладка *Добро пожаловать!*

На рис. 7.3. показан интерфейс выбора объектов архивации в программе Backup.

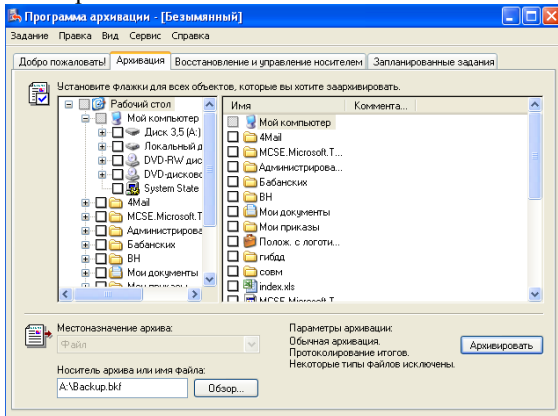


Рис. 7.3. Вкладка *Архивация*

Вкладка *Архивация* позволяет выбрать файлы и папки для архивации. Ресурсы могут находиться на локальных томах или в сетевых папках. Когда папка выбирается целиком, она помечается

синим флажком, если же выбираются только некоторые ресурсы — серым. Для архивации файлов или папок с удаленного компьютера нужно выбрать элементы с сетевого диска или раскрыть окно *Сетевое окружение*. Этот способ более трудоемкий, но и более предпочтительный, поскольку привязки дисков меняются чаще, чем пути UNC. Выбранный список файлов и папок можно сохранить командой *Сохранить выделенные* в меню *Задание*. В дальнейшем его можно загрузить командой *Загрузить выделенные*, чтобы сэкономить время при повторном выборе.

Windows Server 2003 позволяет записывать резервные копии на различные типы носителей: магнитную ленту, сменный диск и в файл на дисковом томе. При использовании магнитной ленты указанное имя должно совпадать с именем ленты в накопителе. При архивации в файл программа Backup создает файл с расширением *.bkf* в указанном размещении. Часто администраторы архивируют данные на каждом сервере и объединяют файлы архивов на центральном сервере, с которого затем данные записываются на сменный носитель. При таком подходе в качестве размещения архива указывается UNC-путь к папке центрального сервера или к локальному файлу на каждом сервере; затем этот архив копируется в центральное размещение.

Программа *Архивация данных* имеет два важных ограничения. Во-первых, она не поддерживает перезаписываемые форматы DVD и CD. Чтобы обойти это ограничение, следует заархивировать данные в файл, а затем скопировать его на DVD- или компакт-диск. Во-вторых, архивация в любое размещение (за исключением файла) требует, чтобы носитель находился в устройстве, физически подключенном к системе.

Стратегии архивирования

Выбрав файлы для архивации и указав размещение резервной копии, нужно выбрать тип архива, определяющий, какие именно из выбранных файлов будут копироваться на целевой носитель.

Каждый тип архива так или иначе связан с атрибутом, который есть у каждого файла, — *Архивный*. Атрибут архивирования — это флаг, который устанавливается при создании или изменении файла. Для уменьшения размера и продолжительности заданий резервного копирования большинство типов архивации записывают на носитель только те файлы, у которых установлен атрибут архивирования.

Существуют следующие типы архивации.

1. Обычная архивация. Архивируются все выбранные файлы и папки. Атрибут *Архивный* сбрасывается. Обычная архивация не учитывает атрибут архивирования при определении файлов,

подлежащих резервному копированию; все выбранные ресурсы записываются на целевой носитель. По сравнению с другими типами обычная архивация выполняется дольше и требует больше места на носителе. Но, поскольку создается полная резервная копия данных, обычная архивация обеспечивает самую высокую скорость восстановления системы. Обычная архивация сбрасывает атрибут архивирования у всех выбранных файлов.

2. Добавочная архивация. На целевой носитель копируются только выбранные файлы с установленным атрибутом архивирования, и флаг сбрасывается. Если добавочная архивация выполняется на следующий день после обычной или другой добавочной архивации, копируются только созданные или измененные за последний день файлы. Добавочная архивация самая быстрая и формирует архив минимального размера. Тем не менее, она не так эффективна, как обычная, поскольку требует восстановления сначала обычного архива, а затем всех последующих добавочных архивов в порядке их создания.

3. Разностная архивация. Копируются только выбранные файлы с атрибутом архивирования, и флаг не сбрасывается. Поскольку разностная архивация учитывает атрибут архивирования, копируются только файлы, созданные или измененные с момента последней обычной или добавочной архивации. Атрибут архивирования не сбрасывается, поэтому разностные архивы содержат не только созданные или измененные файлы, но и все файлы, скопированные при предыдущей разностной архивации. В результате резервные копии становятся больше, а сама разностная архивация длится дольше, чем добавочная, но меньше, чем обычная. Разностная архивация эффективнее добавочной в плане восстановления: требуется восстановить только обычный и последний разностный архивы.

4. Копирующая архивация. Архивируются все выбранные файлы и папки. Атрибут архивирования не учитывается. Копирующая архивация не применяется для обычного или планового резервного копирования. Ее удобно использовать для перемещения данных между системами или создания архивной копии данных на некоторый момент времени без вмешательства в стандартные процедуры резервного копирования.

5. Ежедневная архивация. Копируются все выбранные файлы и папки, измененные в течение дня с момента последней ежедневной архивации (на основе даты изменения файла). Атрибут архивирования не используется и не сбрасывается.

Чтобы выбрать оптимальную стратегию резервного копирования, необходимо учитывать продолжительность и размер задания архивации, а также скорость восстановления системы в случае сбоя. Есть две стратегии архивирования.

1. Обычная и разностная архивация. В воскресенье выполняется обычная архивация, а с понедельника по пятницу — разностная. Разностная архивация не сбрасывает атрибут архивирования, поэтому каждая операция копирует все изменения, произошедшие с понедельника. В случае сбоя данных в пятницу придется восстановить только обычный архив от воскресенья и разностный от четверга. Такая стратегия требует больше времени для резервного копирования, особенно если данные изменяются часто, но восстановление происходит быстрее и удобнее, поскольку набор архивации занимает меньше дисков или лент.

2. Обычная и добавочная архивация. В воскресенье выполняется обычная архивация, а с понедельника по пятницу — добавочная. Последняя сбрасывает атрибут архивирования, поэтому каждая операция архивации включает только файлы, изменившиеся со времени последнего резервного копирования. В случае сбоя данных в пятницу придется восстановить обычный архив, сделанный в воскресенье, и все добавочные архивы с понедельника по пятницу. Такая стратегия требует меньше времени на резервное копирование, но больше на восстановление.

Программа *Архивация данных* позволяет также восстанавливать резервные копии данных. Вкладка *Восстановление и управление носителем* (рис. 7.4) позволяет выбрать набор архивации, с которого нужно восстановить данные. Далее Windows Server 2003 отображает список файлов и папок из набора архивации. Можно выбрать отдельные файлы или папки, которые следует восстановить; синий флажок указывает, что файл или папка будут восстановлены целиком, затененный — что будет восстановлена только часть содержимого папки.

Кроме того, программа предложит указать размещение для восстановления файлов.

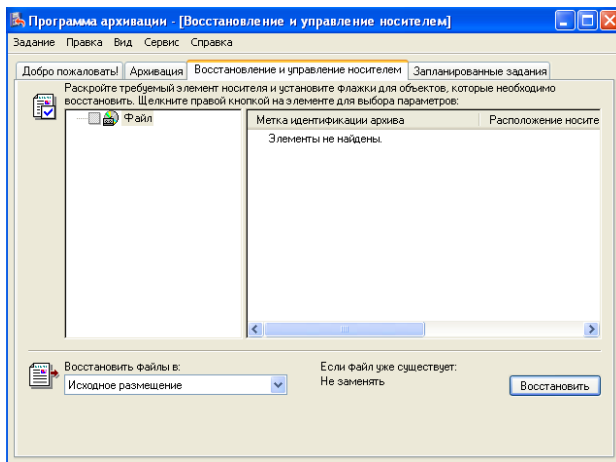


Рис. 7.4. Вкладка *Восстановление и управление носителем*

Можно выбрать один из трех следующих вариантов.

1. Исходное размещение. Данные восстанавливаются в исходную папку, из которой они были архивированы. Исходная структура папки сохраняется или, если папки были удалены, создается заново.
2. Альтернативное размещение. Данные восстанавливаются в папку, указанную в поле *Альтернативное размещение*. Исходная структура папки сохраняется и создается внутри указанной папки, которая считается корнем (томом) архивных данных.
3. Одну папку. Файлы восстанавливаются в указанную папку, но структура папки не сохраняется. Все файлы восстанавливаются в одну папку.

Windows Server 2003 поддерживает несколько параметров, определяющих ход восстановления файлов.

1. Не заменять файл на компьютере. Файлы, которые уже находятся в целевом расположении, пропускаются; этот параметр используется по умолчанию. Такой способ восстановления подходит, когда некоторые файлы удалены из папки, куда идет восстановление. Тогда отсутствующие файлы будут восстановлены из архива.
2. Заменять файл на компьютере, только если он старше. Более свежий файл, который находится в целевой папке, может содержать информацию, которую пользователь не хочет перезаписывать.
3. Всегда заменять файл на компьютере. Все файлы заменяются версией из архива независимо от даты их последнего изменения.

Прежде чем подтвердить восстановление, можно указать, как должны обрабатываться параметры безопасности файлов в архиве. Для этого в диалоговом окне *Подтверждение восстановления* **нужно** щелкнуть *Дополнительно* и установить флажок *Восстановление безопасности*. Если данные архивировались с тома NTFS и восстанавливаются на том NTFS, разрешения, параметры аудита и сведения о владельце будут восстановлены. Если снять этот флажок, данные будут восстанавливаться без дескрипторов безопасности, и все восстановленные файлы будут наследовать разрешения целевой папки или тома.

Дополнительные возможности архивации и восстановления

Windows Server 2003 поддерживает *Службу теневого копирования тома* (Volume Shadow Copy Service, VSS), называемую также *архивацией снимков*. VSS позволяет архивировать БД и другие файлы, которые открыты или заблокированы действиями пользователей или системы. Теневое копирование позволяет приложениям продолжать записывать данные на том во время резервного копирования, а администраторам — выполнять архивацию в любое время, не прерывая работу пользователей и не рискуя пропустить файлы.

Чтобы заархивировать или восстановить файл, необходимо обладать пользовательскими правами *Архивация файлов и каталогов* и *Восстановление файлов и каталогов* или NTFS-разрешениями *Чтение* и *Запись* в целевом размещении. Такими привилегиями обладают группы *Администраторы* и *Операторы архива*, поэтому, чтобы предоставить учетной записи пользователя, группы или службы минимальные требуемые привилегии, нужно добавить ее в группу *Операторы архива* на сервере. Пользователи с правом *Восстановление файлов и каталогов* могут удалять NTFS-разрешения с файлов при восстановлении. В Windows Server 2003 они также могут передавать право владения файлами другим пользователям.

Также программа *Архивация данных* в Windows Server 2003 тесно взаимодействует со службой RSM. Эта служба, разработанная для управления автоматическими библиотеками лент и приводами CD-ROM, принимает от других служб или приложений запросы к носителю и гарантирует, что он правильно смонтирован и загружен.

RSM также позволяет работать с устройствами, куда вручную загружается один носитель, например, с ленточными накопителями, приводами CD-ROM или Iomega Jaz. При работе с такими устройствами RSM отслеживает носители по меткам или серийным

номерам, и даже в системе архивации с одним носителем у каждой ленты должна быть уникальная метка.

Программа *Архивация данных* в Windows Server 2003 управляет лентами через службу RSM, используя пулы носителей (рис. 7.5).

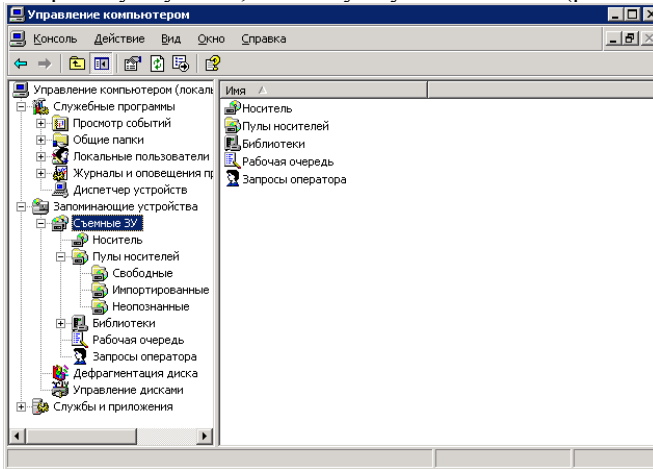


Рис. 7.5. Пулы носителей

С архивацией связаны следующие пулы носителей.

1. Неопознанные. Содержит полностью чистые или отформатированные в неизвестном формате ленты.
2. Свободные. Содержит только вновь отформатированные ленты плюс те, что администратор специально пометил свободными. Свободные носители перемещаются в архивный пул, когда на них записывают набор архивации.
3. Backup. Содержит носители, записанные программой Архивация данных (Backup), которая архивирует только на носитель в свободном пуле, а также на носитель в архивном пуле с указанным именем.
4. Импортированные. Содержит ленты, не каталогизированные на локальном диске. При создании каталога такая лента перемещается в архивный пул.

Одновременно с набором архивации программа *Архивация данных* создает каталог со списком файлов и папок из этого набора. Такой каталог хранится на диске сервера и называется локальным или дисковым каталогом, а также в наборе архивации и называется каталогом на носителе. Он облегчает быстрый поиск файлов и папок, подлежащих восстановлению. Программа *Архивация данных* может

отобразить каталог мгновенно, а не загружать его с медленного архивного носителя. Каталог на носителе используется, если локальный каталог выходит из строя или когда файлы передаются в другую систему. В этом случае Windows создает локальный каталог из копии на носителе.

Вкладка *Восстановление и управление носителем* позволяет выполнять следующие операции над каталогами.

1. Удаление. Если потерялся или повредился носитель архива или файлы были перемещены в другую систему и локальный каталог больше не нужен, щелкните набор архивации правой кнопкой и выберите *Удалить каталог*. Эта команда не удаляет каталог на носителе.

2. Пополнение. Некаталогизированная на локальном компьютере лента из другой системы появится в импортированном пуле носителей. Щелкните носитель правой кнопкой и выберите *Каталог*. Windows скопирует локальный каталог с ленты или из файла. Эта операция не создает и не изменяет каталог на носителе.

На вкладке *Общие* диалогового окна *Параметры* можно настроить следующие параметры архивации.

1. Оценивать информацию о выборе файлов перед выполнением операций архивации или восстановления. Программа *Архивация данных* перед началом операции подсчитывает количество и размер файлов.

2. Использовать каталоги носителей для ускорения построения каталогов восстановления на диске. Позволяет создать локальный каталог для ленты из каталога на носителе. Однако если ленты с каталогом на носителе нет или носитель в наборе поврежден, вы можете снять этот флажок, и система просмотрит весь набор архивации чтобы построить каталог на диске. Если набор архивации большой, такая операция может занять несколько часов.

3. Проверять данные после завершения архивации. Система сравнивает содержимое носителя архива с исходными файлами и фиксирует любые отличия. Этот параметр сильно замедляет архивацию. Расхождения обычно появляются, когда данные часто меняются в процессе резервного копирования или проверки, поэтому не рекомендуется проверять архивы системы, поскольку системные файлы постоянно меняются.

4. Архивировать содержимое подключенных дисков. Подключенный диск — это дисковый том, спроецированный на папку в пространстве имен другого тома, а не на букву диска. Если этот флажок сброшен, архивируется только путь к папке, подключенной к

тому, но не ее содержимое. Если же флажок установлен, архивируется также содержимое подключенного тома.

Диалоговое окно *Параметры* содержит вкладку *Журнал архивации*. В журнале регистрируются проблемы, угрожающие жизнеспособности резервной копии. Рекомендуется вести только сводный журнал (это вариант по умолчанию), который содержит сведения о пропущенных файлах и ошибках.

Система хранит 10 журналов архивации в каталоге %UserProfile%\Local Settings\ApplicationData\Microsoft\Windows NT\Ntbackup\Data. Путь и максимальное количество хранимых журналов изменить нельзя.

Вкладка *Исключение файлов* диалогового окна *Параметры* позволяет указать расширения и отдельные файлы, которые следует пропустить при архивации. По умолчанию программа *Архивация данных* пропускает файл подкачки, временные файлы, кэш на стороне клиента, папку отладки, базу данных и папки *Службы репликации файлов*, а также другие локальные журналы и БД. Файлы можно исключить в зависимости от их владельца.

Выбрав файлы и запустив резервное копирование кнопкой *Архивировать*, можно настроить дополнительные параметры для конкретного задания, щелкнув кнопку *Дополнительно*:

1. Проверять данные после архивации. Перекрывает значение по умолчанию, указанное в диалоговом окне *Параметры* программы *Архивация данных*;

2. Если возможно, сжимать архивируемые данные. Включает сжатие данных для экономии места на носителе архива; недоступен, если ленточный накопитель не поддерживает сжатие;

3. Отключить теневое копирование состояния тома. Если этот флажок установлен, некоторые открытые или используемые файлы могут быть пропущены.

Команда Ntbackup позволяет создавать сценарии заданий архивации. Ее синтаксис таков:

```
ntbackup backup [systemstate] "@имя_файла_bks" /J
{"имя_задания"} [/P {"имя_пула"}] [/G {"идентификатор_guid"}]
[/T { "имя_ленты"}] [/N {"носитель"}] [/F {"имя_файла"}] [/D
{"описание"}] [/DS {"имя_сервера"}] [/LS {"имя_сервера"}] [/A] [/V:
{yes|no}] [/R:{yes|no}] [/L:{f|s|n}] [/M {тип_архива}] [/RS:{yes|no}]
[/HC:{on|off}] [/SNAP:{on|off}]
```

Параметр *backup* задает рабочий режим: нельзя восстановить данные из командной строки. За ним следует параметр, указывающий, что именно нужно архивировать. Можно указать путь к локальной

папке, сетевому общему ресурсу, файлу. Кроме того, можно указать путь к файлу выбора архивации (с расширением .bks), используя синтаксис *@имя_файла_bks* (перед именем файла выбора архивации должен стоять символ @). Этот файл содержит информацию о файлах и папках, подлежащих архивации, и должен быть создан из графического интерфейса программы *Архивация данных*.

Параметр, /J *«имя_задания»*, указывает описательное имя задания, которое используется в отчете архивации.

Параметр /F *«имя_файла»*, где *имя_файла* — полное имя файла, содержащее путь к логическому диску. Не используется с параметрами /T, /P, /G.

Параметр /A используется для выполнения операции дозаписи. При дозаписи на ленту, а не в файл, с этим параметром необходимо использовать параметры /G или /T. Не используется с параметрами /N или /P.

Параметр /N *«имя_носителя»* используется для архивации на новую ленту или в файл, где *имя_носителя* — имя новой ленты. Не используется с параметром /A.

Параметр /P *«имя_пула»* используется для архивации на новую ленту, где *имя_пула* — пул, содержащий архивный носитель. Не используется с параметрами /A, /G, /F или /T.

Чтобы указать ленту для операции дозаписи или перезаписи, используются параметр /T или /G вместе с /A (дозапись) или /N (перезапись). Параметр /P нельзя использовать с параметрами /T или /G.

Чтобы указать имя ленты, используется параметр /T *«имя_ленты»*, где *имя_ленты* — действительная лента в пуле носителей.

Чтобы указать ленту по идентификатору GUID, а не по имени, используется параметр /G *«имя_GUID»*, где *имя_GUID* — действительная лента в пуле носителей.

Параметр /M *{тип_архивации}* — указывает один из следующих типов архивации: *обычная* (normal), *копирующая* (copy), *разностная* (differential), *добавочная* (incremental) или *ежедневная* (daily).

Параметр /D *«описание_набора»* — указывает метку для набора архивации.

Параметр /V:{yes | no} — проверяет данные по завершении архивации.

Параметр /R:{yes | no} — разрешает доступ к ленте только владельцам и членам группы *Администраторы*.

Параметр /L:{f | s | n} — указывает тип файла журнала: f — полный (full), s — сводный (summary), n — журнал не создается (none).

Параметр /RS:{yes | no} — архивирует перенесенные файлы данных, расположенные в узле *Съемные ЗУ*.

Параметр /HC:{on | off} — включает аппаратное сжатие на ленточном накопителе, если оно поддерживается.

Параметр /SNAP: {on | off} — указывает программе архивации использовать теневое копирование тома.

Планирование заданий архивации

Для архивации по расписанию нужно создать задание архивации в программе *Архивация данных*, щелкнуть *Архивировать* и настроить дополнительные параметры. Затем щелкнуть кнопку *Расписание* и в окне *Указание учетной записи* ввести имя пользователя и пароль учетной записи, которая будет использоваться заданием архивации.

Рекомендуется создавать учетную запись для каждой службы. Службу не следует запускать под учетной записью пользователя или от имени *Администратор*. Если пароль учетной записи пользователя изменится, придется изменить настройки для всех служб, которые запускаются в ее контексте. Учетная запись для задания архивации должна быть включена в группу *Операторы архива*.

В окне *Параметры запланированного задания* следует ввести имя задания и щелкнуть *Свойства*. Откроется окно *Запланированное задание*, показанное на рис. 7.6.

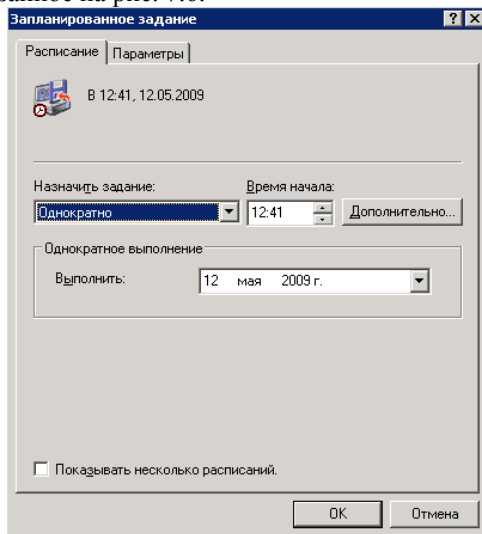


Рис. 7.6. Диалоговое окно *Запланированное задание*

Нужно настроить дату, время и периодичность задания. Кнопка *Дополнительно* позволяет настроить дополнительные параметры расписания, включая диапазон дат, когда следует выполнять задание. Вкладка *Параметры* окна *Запланированное задание* позволяет точнее описать задание, например, указать, что оно должно выполняться, если компьютер простаивает в течение указанного интервала времени.

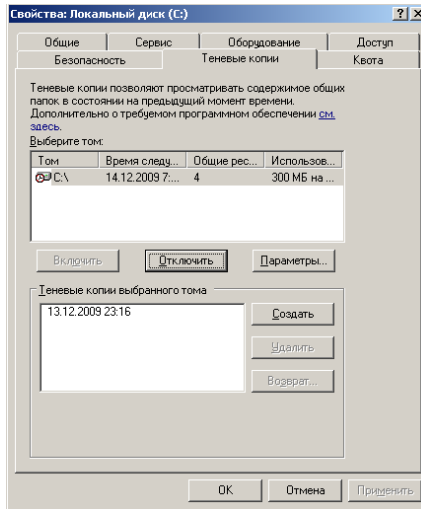
Составленное расписание можно редактировать на вкладке *Запланированные задания* программы *Архивация данных*. Если щелкнуть в календаре задание, откроется его расписание. Кроме того, можно добавить задание архивации, щелкнув кнопку *Добавить задание* на вкладке *Запланированные задания*: запустится мастер архивации, позволяющий выбрать файлы, подлежащие архивации, и указать другие свойства задания.

Теневые копии общих папок

Используя теневое копирование томов (VSS), Windows Server 2003 автоматически кэширует копии файлов по мере их изменения. Если пользователь удаляет, перезаписывает или нежелательно изменяет файл, можно просто восстановить его предыдущую версию. Тем не менее, эта важная функция не исключает архивацию. Она обеспечивает быстрое восстановление при решении простых, повседневных проблем, но не предназначена для восстановления больших объемов потерянных данных.

Функция *Теневые копии* для общих папок по умолчанию отключена. Чтобы включить ее, нужно открыть окно свойств дискового тома в *Проводнике* или в оснастке *Управление дисками*. На вкладке *Теневые копии*, показанной на рис. 7.7, выбрать том и щелкнуть *Включить*. После включения будут созданы теневые копии для всех общих папок на данном томе; отдельные общие папки на томе выбрать нельзя.

Если щелкнуть *Отключить*, все копии, созданные службой VSS, будут удалены. По умолчанию сервер создает копии общих папок с понедельника по пятницу в 7:00 и в полдень. При этом для кэширования теневых копий используется 10 % пространства на том диске, где находится общая папка.

Рис. 7.7. Вкладка *Теневые копии*

Щелкнув кнопку *Параметры* на вкладке *Теневые копии*, можно настроить следующие параметры.

1. Место хранения. Чтобы повысить производительность, можно переместить теневое хранилище на другой том. Это нужно сделать, когда никакие теневые копии еще не созданы, в противном случае их придется удалить.

2. Сведения. Если щелкнуть эту кнопку, откроется одноименную диалоговое окно, где перечислены теневые копии и занимаемое ими пространство.

3. Ограничения хранилища. Не может быть менее 100 Мб. Когда размер теневой копии превышает указанное ограничение, старые версии файлов удаляются, освобождая место для новых версий. Оптимальное значение этого параметра зависит от суммарного размера общих папок на томе; частоты изменения файлов, размера этих файлов и количества предыдущих версий, которые нужно хранить. В любом случае до момента удаления самой старой версии из теневого хранилища можно сохранить не более 63 версий файла.

4. Расписание. Позволяет настроить расписание, отражающее график работы пользователей, чтобы гарантировать хранение достаточного количества версий файлов и чтобы место хранения не заполнилось преждевременно, вызвав удаление старых версий. Помните, что, когда создается теневая копия, копируются любые файлы, измененные с момента последнего теневого копирования. Если

файлы изменились несколько раз между созданием теневых копий, промежуточные версии будут недоступны.

Теневые копии общих папок позволяют получить доступ к предыдущим версиям файлов, которые сервер кэширует по заданному расписанию. Это позволит:

- восстановить случайно удаленные файлы;
- восстановить случайно перезаписанный файл;
- сравнить версии файлов во время работы.

Чтобы получить предыдущие версии, нужно открыть окно свойств папки или файла и перейти на вкладку *Предыдущие версии*, показанную на рис. 7.8.

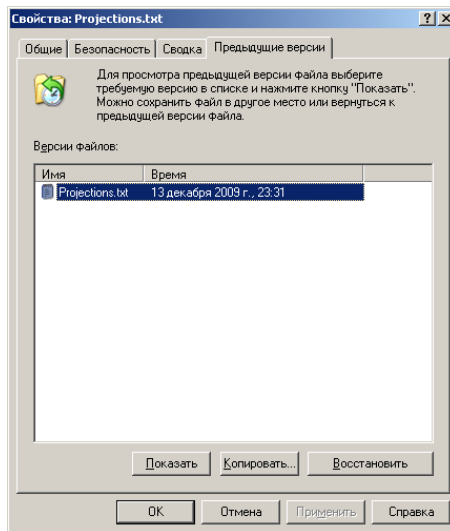


Рис. 7.8. Вкладка *Предыдущие версии*

Вкладка *Предыдущие версии* недоступна, если функция *Теневые копии* отключена на сервере или на нем не были сохранены предыдущие версии. Кроме того, она недоступна, если на компьютере не был установлен клиент теневого копирования. Файл клиента находится в папке %Systemroot%\System32\Clients\Twclient\x86 на системе Windows Server 2003. Файл Windows Installer (.msi) можно развернуть, используя групповую политику, пакет SMS или электронную почту. Также, вкладка *Предыдущие версии* доступна при обращении к свойствам файлов через общую папку. Кнопка

Восстановить позволяет восстановить файл в предыдущее размещение, а кнопка *Копировать* — в новое.

В отличие от полноценной операции восстановления, теневое копирование не поддерживает восстановление параметров безопасности предыдущих версий файлов. Если восстанавливается файл в исходное размещение, и он там уже существует, предыдущая версия заменяет текущую со своими разрешениями. Когда предыдущая версия файла копируется в другое место или восстанавливается в исходное, но такого файла там нет, предыдущая версия наследует разрешения от родительской папки.

Теневое копирование является полезным дополнением к набору средств для управления файловыми серверами и общими данными. С помощью VSS можно защитить наборы данных в состоянии на запланированные моменты времени. Администраторы и пользователи могут восстанавливать удаленные или поврежденные файлы, а также сравнивать файлы с предыдущими версиями. По мере заполнения кэша VSS старые версии заменяются новыми теневыми копиями. Если сервер вышел из строя или пользователю нужны данные, которые уже недоступны на вкладке *Предыдущие версии*, их можно восстановить из архива. Хотя VSS улучшает управление общими файлами и надежность их хранения, альтернативы тщательно спланированной и проверенной процедуре резервного копирования нет.

Заключение

В данном пособии были рассмотрены основы администрирования серверов под управлением Windows Server 2003, приложений, сетевых и информационных сервисов и информационных сетей. Были изучены методы, средства и формы административного управления в информационных системах.

Особое внимание было уделено методам решения конкретных задач системного администрирования на основе современных стандартов, использованию инструментальных средств поддержки административного управления для оперативного управления и обслуживания технических средств.

Кроме того, были рассмотрены вопросы управления учетными записями пользователей, групп, компьютеров, управления файлами, папками, управления резервным копированием данных.

Пособие заканчивается подробным рассмотрением вопросов планирования эффективных стратегий архивирования и восстановления данных.

Библиографический список

1. Закер, Крейг. Официальный учебный курс Microsoft: Управление и поддержка среды Microsoft Windows Server 2003 (70-290) / К. Закер; пер. с англ. - М.: ЭКОМ; БИНОМ. Лаборатория знаний, 2006. - 447 с.: ил.
2. Клейменов, С.А. Администрирование в информационных системах: учеб. пособие для студ. высш. учеб. заведений / С.А. Клейменов, В.П. Мельников, А.М. Петраков; под ред. В.П. Мельникова. - М.: Издательский центр «Академия», 2008. - 272 с.
3. Коробко, И. В. Администрирование сетей Windows с помощью сценариев / И.В. Коробко. - СПб.: БХВ-Петербург, 2007.
4. Коробко, И. В. Справочник системного администратора по программированию Windows/ И.В. Коробко. - СПб.: БХВ-Петербург, 2009. - 576 с.: ил.
5. Макин, Дж. С. Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. Учебный курс Microsoft / Дж. С. Макин, Йен Маклин. Пер.с англ. — 2-е изд., испр. - М.: «Русская Редакция»; СПб.: Питер, 2008. - 624 стр.: ил.
6. Самойленко, А. Виртуальные машины на платформе Microsoft Virtual PC 2007 / А. Самойленко [Электронный ресурс] - Режим доступа: <http://www.windowsfaq.ru/content/view/566>
7. Семенов, Ю.А. Протокол LDAP (Lightweight Directory Access Protocol) / Ю.А. Семенов [Электронный ресурс] - Режим доступа: <http://book.itep.ru/4/45/ldap.htm>
8. Хенриксон, Х. IIS 6.0. Полное руководство. Справочник профессионала. /Х. Хенриксон, С. Хофман. Пер. с англ., - М.: Издательство «СП ЭКОМ», 2004. - 672 с.: ил.
9. Холме, Дэн. Управление и поддержка Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Холме Дэн, Томас Орин. Пер. с англ. — М.: Издательско-торговый дом «Русская Редакция», 2008. — 448 стр.: ил.
10. Чекмарев, А. Н. Microsoft Windows Server 2003. Русская версия / Чекмарев А.Н., Вишневецкий А.В., Кокорева О.И. Под общ. ред. А.Н. Чекмарева. - СПб.: БХВ-Петербург, 2008. - 1120 с.: ил.

Учебное издание

Федотов Евгений Александрович

АДМИНИСТРИРОВАНИЕ ПРОГРАММНЫХ И ИНФОРМАЦИОННЫХ СИСТЕМ

Подписано в печать ~~30.10.12~~. Формат 60х84/16. Усл. печ. л. 7,8. Уч.-изд. л. 8,4.
Тираж ~~77~~ экз. Заказ Цена
Отпечатано в Белгородском государственном технологическом университете
им. В.Г. Шухова
308012, г. Белгород, Костюкова, 46