Современные сети часто состоят из множества различных программных платформ, большого разнообразия оборудования и программного обеспечения. Пользователи зачастую вынуждены запоминать большое количество паролей для доступа к различным сетевым ресурсам. Права доступа могут быть различными для одного и того же сотрудника в зависимости от того, с какими ресурсами он работает. Все это множество взаимосвязей требует от администратора и пользователя огромного количества времени на анализ, запоминание и обучение.

Решение проблемы управления такой разнородной сетью было найдено с разработкой службы каталога. Службы каталога предоставляют возможности управления любыми ресурсами и сервисами из любой точки независимо от размеров сети, используемых операционных систем и сложности оборудования. Информация о пользователе, заносится единожды в службу каталога, и после этого становится доступной в пределах всей сети. Адреса электронной почты, принадлежность к группам, необходимые права доступа и учетные записи для работы с различными операционными системами — все это создается и поддерживается в актуальном виде автоматически. Любые изменения, занесенные в службу каталога администратором, сразу обновляются по всей сети. Администраторам уже не нужно беспокоиться об уволенных сотрудниках — просто удалив учетную запись пользователя из службы каталога, он сможет гарантировать автоматическое удаление всех прав доступа на ресурсы сети, предоставленные ранее этому сотруднику.

В настоящее время большинство служб каталогов различных фирм базируются на стандарте *X.500*. Для доступа к информации, хранящейся в службах каталогов, обычно используется протокол *Lightweight Directory Access Protocol* ( *LDAP* ). В связи со стремительным развитием сетей TCP/IP, протокол LDAP становится стандартом для служб каталогов и приложений, ориентированных на использование службы каталога.

Служба каталогов Active Directory является основой логической структуры корпоративных сетей, базирующихся на системе Windows. Термин " *Каталог* " в самом широком смысле означает " *Справочник* ", а служба каталогов корпоративной сети — это централизованный корпоративный справочник. Корпоративный каталог может содержать информацию об объектах различных типов. Служба каталогов Active Directory содержит в первую очередь объекты, на которых базируется система безопасности сетей Windows, — учетные записи пользователей, групп и компьютеров. Учетные записи организованы в логические структуры: *домен, дерево*, лес, организационные подразделения.

С точки зрения изучения материала курса "Сетевое администрирование" вполне возможен следующий вариант прохождения учебного материала: сначала изучить первую часть данного раздела (от основных понятий до установки контроллеров домена), затем перейти к Разделу 8 "Служба файлов и печати", а после изучения 8-го раздела вернуться кразделу 6 для изучения более сложных понятий служб каталогов.

**6.1 Основные термины и понятия (лес, дерево, домен, организационное подразделение). Планирование пространства имен AD. Установка контроллеров доменов**

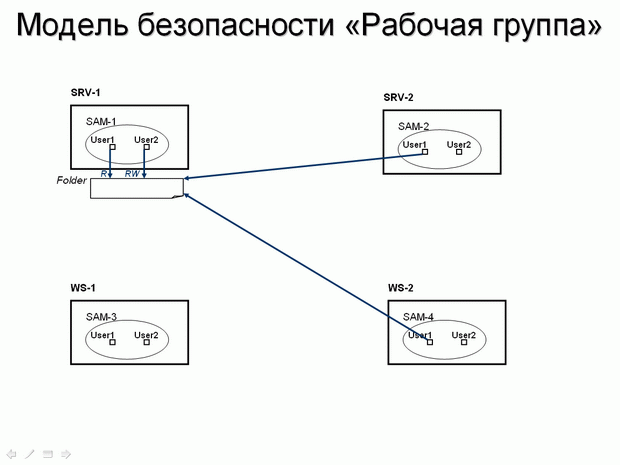
**Модели управления безопасностью: модель "Рабочая группа" и централизованная доменная модель**

Как уже говорилось выше, основное назначение служб каталогов — управление сетевой безопасностью. Основа сетевой безопасности — база данных учетных записей (accounts) пользователей, групп пользователей и компьютеров, с помощью которой осуществляется управление доступом к сетевым ресурсам. Прежде чем говорить о службе каталогов Active Directory, сравним две модели построения базы данных служб каталогов и управления доступом к ресурсам.

**Модель "Рабочая группа"**

Данная модель управления безопасностью корпоративной сети — самая примитивная. Она предназначена для использования в небольших *одноранговых сетях* (3–10 компьютеров) и основана на том, что каждый компьютер в сети с операционными системами Windows NT/2000/XP/2003 имеет свою собственную локальную базу данных учетных записей и с помощью этой *локальной БД* осуществляется управление доступом к ресурсам данного компьютера. *Локальная БД*учетных записей называется база данных *SAM* ( *Security Account Manager* ) и хранится в реестре операционной системы. Базы данных отдельных компьютеров полностью изолированы друг от друга и никак не связаны между собой.

Пример управления доступом при использовании такой модели изображен на рис. 6.1.



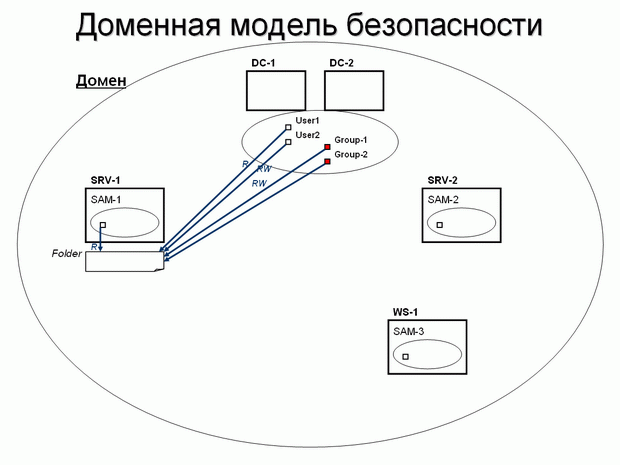
**Рис. 6.1.**

В данном примере изображены два сервера (SRV-1 и SRV-2) и две рабочие станции (WS-1 и WS-2). Их базы данных SAM обозначены соответственно SAM-1, SAM-2, SAM-3 и SAM-4 (на рисунке базы SAM изображены в виде овала). В каждой БД есть учетные записи пользователей User1 и User2. Полное имя пользователя User1 на сервере SRV-1 будет выглядеть как "SRV-1\User1", а полное имя пользователя User1 на рабочей станции WS-1 будет выглядеть как "WS-1\User1". Представим, что на сервере SRV-1 создана папка Folder, к которой предоставлен доступ по сети пользователям User1 — на чтение (R), User2 — чтение и запись (RW). Главный момент в этой модели заключается в том, что компьютер SRV-1 ничего "не знает" об учетных записях компьютеров SRV-2, WS-1, WS-2, а также всех остальных компьютеров сети. Если пользователь с именем User1локально зарегистрируется в системе на компьютере, например, WS-2 (или, как еще говорят, "войдет в систему с локальным именем User1 на компьютере WS-2"), то при попытке получить доступ с этого компьютера по сети к папке Folder на сервере SRV-1 сервер запросит пользователя ввести имя и пароль (исключение составляет тот случай, если у пользователей с одинаковыми именами одинаковые пароли).

Модель "Рабочая группа" более проста для изучения, здесь нет необходимости изучать сложные понятия Active Directory. Но при использовании в сети с большим количеством компьютеров и сетевых ресурсов становится очень сложным управлять именами пользователей и их паролями — приходится на каждом компьютере (который предоставляет свои ресурсы для совместного использования в сети) вручную создавать одни и те же учетные записи с одинаковыми паролями, что очень трудоемко, либо делать одну учетную запись на всех пользователей с одним на всех паролем (или вообще без пароля), что сильно снижает уровень защиты информации. Поэтому модель "Рабочая группа" рекомендуется только для сетей с числом компьютеров от 3 до 10 (а еще лучше — не более 5), при условии что среди всех компьютеров нет ни одного с системой Windows Server.

**Доменная модель**

В доменной модели существует единая база данных служб каталогов, доступная всем компьютерам сети. Для этого в сети устанавливаются специализированные серверы, называемые *контроллерами домена*, которые хранят на своих жестких дисках эту базу. На рис. 6.2. изображена схема доменной модели. Серверы DC-1 и DC-2 — контроллеры домена, они хранят доменную базу данных учетных записей (каждый контроллер хранит у себя свою собственную копию БД, но все изменения, производимые в БД на одном из серверов, реплицируются на остальные контроллеры).



**Рис. 6.2.**

В такой модели, если, например, на сервере SRV-1, являющемся членом домена, предоставлен общий доступ к папке Folder, то права доступа к данному ресурсу можно назначать не только для учетных записей локальной базы SAM данного сервера, но, самое главное, учетным записям, хранящимся в доменной БД. На рисунке для доступа к папке Folder даны права доступа одной локальной учетной записи компьютера SRV-1 и нескольким учетным записям домена (пользователя и группам пользователей). В доменной модели управления безопасностью пользователь регистрируется на компьютере ("входит в систему") со своей *доменной учетной записью* и, независимо от компьютера, на котором была выполнена регистрация, получает доступ к необходимым сетевым ресурсам. И нет необходимости на каждом компьютере создавать большое количество локальных учетных записей, все записи созданы *однократно в доменной БД*. И с помощью доменной базы данных осуществляется *централизованное управление доступом* к сетевым ресурсам *независимо от количества компьютеров в сети*.

**Назначение службы каталогов Active Directory**

Каталог (справочник) может хранить различную информацию, относящуюся к пользователям, группам, компьютерам, сетевым принтерам, общим файловым ресурсам и так далее — будем называть все это объектами. Каталог хранит также информацию о самом объекте, или его свойства, называемые атрибутами. Например, атрибутами, хранимыми в каталоге о пользователе, может быть имя его руководителя, номер телефона, адрес, имя для входа в систему, *пароль, группы*, в которые он входит, и многое другое. Для того чтобы сделать хранилище каталога полезным для пользователей, должны существовать службы, которые будут взаимодействовать с каталогом. Например, можно использовать каталог как хранилище информации, по которой можно аутентифицировать пользователя, или как место, куда можно послать запрос для того, чтобы найти информацию об объекте.

Active Directory отвечает не только за создание и организацию этих небольших объектов, но также и за большие объекты, такие как домены, OU (организационные подразделения) и сайты.

Об основных терминах, используемых в контексте службы каталогов Active Directory, читайте ниже.

Служба каталогов Active Directory (сокращенно — AD) обеспечивает эффективную работу сложной корпоративной среды, предоставляя следующие возможности:

* *Единая регистрация в сети* ; Пользователи могут регистрироваться в сети с одним именем и паролем и получать при этом доступ ко всем сетевым ресурсам и службам (службы сетевой инфраструктуры, службы файлов и печати, серверы приложений и баз данных и т. д.);
* *Безопасность информации*. Средства аутентификации и управления доступом к ресурсам, встроенные в службу Active Directory, обеспечивают централизованную защиту сети;
* *Централизованное управление*. Администраторы могут централизованно управлять всеми корпоративными ресурсами;
* *Администрирование с использованием групповых политик*. При загрузке компьютера или регистрации пользователя в системе выполняются требования групповых политик; их настройки хранятся в *объектах групповых политик* (*GPO*) и применяются ко всем учетным записям пользователей и компьютеров, расположенных в сайтах, доменах или организационных подразделениях;
* *Интеграция с DNS*. Функционирование служб каталогов полностью зависит от работы службы DNS. В свою очередь серверы DNS могут хранить информацию о зонах в базе данных Active Directory;
* *Расширяемость каталога*. Администраторы могут добавлять в схему каталога новые классы объектов или добавлять новые атрибуты к существующим классам;
* *Масштабируемость*. Служба Active Directory может охватывать как один домен, так и множество доменов, объединенных в дерево доменов, а из нескольких деревьев доменов может быть построен лес;
* *Репликация информации*. В службе Active Directory используется репликация служебной информации в схеме со многими ведущими ( *multi-master* ), что позволяет модифицировать БД Active Directory на любом контроллере домена. Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость и возможность распределения сетевой нагрузки;
* *Гибкость запросов к каталогу*. БД Active Directory может использоваться для быстрого поиска любого объекта AD, используя его свойства (например, имя пользователя или адрес его электронной почты, тип принтера или его местоположение и т. п.);
* *Стандартные интерфейсы программирования*. Для разработчиков программного обеспечения служба каталогов предоставляет доступ ко всем возможностям (средствам) каталога и поддерживает принятые стандарты и интерфейсы программирования (API).

В Active Directory может быть создан широкий круг различных объектов. Объект представляет собой уникальную сущность внутри Каталога и обычно обладает многими атрибутами, которые помогают описывать и распознавать его. Учетная запись пользователя является примером объекта. Этот тип объекта может иметь множество атрибутов, таких как имя, фамилия, пароль, номер телефона, адрес и многие другие. Таким же образом общий принтер тоже может быть объектом в Active Directory и его атрибутами являются его имя, местоположение и т.д. Атрибуты объекта не только помогают определить объект, но также позволяют вам искать объекты внутри Каталога.

**Терминология**

Служба каталогов системы Windows Server построена на общепринятых технологических стандартах. Изначально для служб каталогов был разработан стандарт*X.500*, который предназначался для построения иерархических древовидных масштабируемых справочников с возможностью расширения как классов объектов, так и наборов атрибутов (свойств) каждого отдельного класса. Однако практическая реализация этого стандарта оказалась неэффективной с точки зрения производительности. Тогда на базе стандарта X.500 была разработана упрощенная (облегченная) версия стандарта построения каталогов, получившая название*LDAP* ( *Lightweight Directory Access Protocol* ). Протокол LDAP сохраняет все основные свойства X.500 (иерархическая система построения справочника, масштабируемость, расширяемость), но при этом позволяет достаточно эффективно реализовать данный стандарт на практике. Термин " *lightweight* " ("*облегченный*") в названии LDAP отражает основную цель разработки протокола: создать инструментарий для построения службы каталогов, которая обладает достаточной функциональной мощью для решения базовых задач, но не перегружена сложными технологиями, делающими реализацию служб каталогов неэффективной. В настоящее время LDAP является стандартным методом доступа к информации сетевых каталогов и играет роль фундамента во множестве продуктов, таких как системы аутентификации, почтовые программы и приложения электронной коммерции. Сегодня на рынке присутствует более 60 коммерческих серверов LDAP, причем около 90% из них представляют собой самостоятельные серверы каталогов LDAP, а остальные предлагаются в качестве компонентов других приложений.

Протокол LDAP четко определяет круг операций над каталогами, которые может выполнять клиентское приложение. Эти операции распадаются на пять групп:

* установление связи с каталогом;
* поиск в нем информации;
* модификация его содержимого;
* добавление объекта;
* удаление объекта.

Кроме протокола LDAP служба каталогов Active Directory использует также протокол аутентификации *Kerberos* и службу DNS для поиска в сети компонент служб каталогов (контроллеры доменов, *серверы глобального каталога*, службу Kerberos и др.).

**Домен**

Основной единицей системы безопасности Active Directory является *домен*. Домен формирует область административной ответственности. База данных домена содержит учетные записи *пользователей*, *групп* и *компьютеров*. Большая часть функций по управлению службой каталогов работает на уровне домена (аутентификация пользователей, управление доступом к ресурсам, управление службами, управление репликацией, политики безопасности).

Имена доменов Active Directory формируются по той же схеме, что и имена в пространстве имен DNS. И это не случайно. Служба DNS является средством поиска компонент домена — в первую очередь контроллеров домена.

*Контроллеры домена* — специальные серверы, которые хранят соответствующую данному домену часть базы данных Active Directory. Основные функции контроллеров домена:

* **хранение БД Active Directory** (организация доступа к информации, содержащейся в каталоге, включая управление этой информацией и ее модификацию);
* **синхронизация изменений в AD** (изменения в базу данных AD могут быть внесены на любом из контроллеров домена, любые изменения, осуществляемые на одном из контроллеров, будут синхронизированы c копиями, хранящимися на других контроллерах);
* **аутентификация пользователей** (любой из контроллеров домена осуществляет проверку полномочий пользователей, регистрирующихся на клиентских системах).

Настоятельно рекомендуется в каждом домене устанавливать не менее двух контроллеров домена — во-первых, для защиты от потери БД Active Directory в случае выхода из строя какого-либо контроллера, во-вторых, для распределения нагрузки между контроллерами.

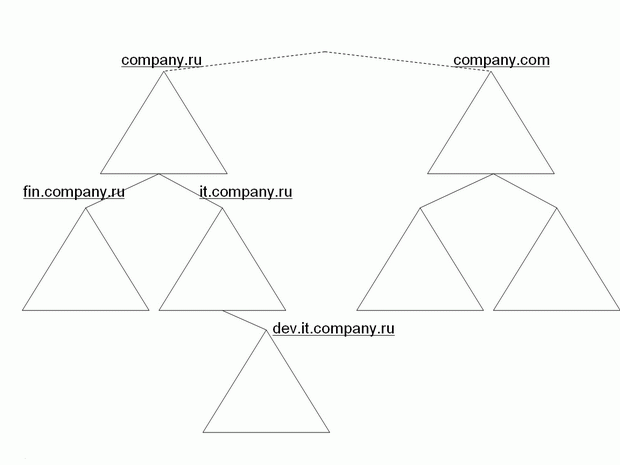
**Дерево**

Дерево является набором доменов, которые используют единое связанное пространство имен. В этом случае "дочерний" домен наследует свое имя от "родительского" домена. Дочерний домен автоматически устанавливает двухсторонние транзитивные доверительные отношения с родительским доменом. Доверительные отношения означают, что ресурсы одного из доменов могут быть доступны пользователям других доменов.

Пример дерева Active Directory изображен на рис. 6.3. В данном примере домен company.ru является доменом Active Directory верхнего уровня. От корневого домена отходят дочерние домены it.company.ru и fin.company.ru. Эти домены могут относиться соответственно к ИТ-службе компании и финансовой службе. У домена it.company.ru есть поддомен dev.it.company.ru, созданный для отдела разработчиков ПО ИТ-службы.

Корпорация Microsoft рекомендует строить Active Directory в виде одного домена. Построение дерева, состоящего из многих доменов необходимо в следующих случаях:

* для децентрализации администрирования служб каталогов (например, в случае, когда компания имеет филиалы, географически удаленные друг от друга, и централизованное управление затруднено по техническим причинам);
* для повышения производительности (для компаний с большим количеством пользователей и серверов актуален вопрос повышения производительности работы контроллеров домена);
* для более эффективного управления репликацией (если контроллеры доменов удалены друг от друга, то репликация в одном может потребовать больше времени и создавать проблемы с использованием несинхронизированных данных);
* для применения различных политик безопасности для различных подразделений компании;
* при большом количестве объектов в БД Active Directory.



**Рис. 6.3.**

**Лес**

Наиболее крупная структура в Active Directory. Лес объединяет деревья, которые поддерживают единую схему ( *схема Active Directory*— набор определений типов, или классов, объектов в БД Active Directory). В лесу между всеми доменами установлены двухсторонние транзитивные доверительные отношения, что позволяет пользователям любого домена получать доступ к ресурсам всех остальных доменов, если они имеют соответствующие разрешения на доступ. По умолчанию, первый домен, создаваемый в лесу, считается его корневым доменом, в корневом домене хранится схема AD.

Новые деревья в лесу создаются в том случае, когда необходимо построить иерархию доменов с пространством имен, отличным от других пространств леса. В примере на рис. 6.3 российская компания могла открыть офис за рубежом и для своего зарубежного отделения создать дерево с доменом верхнего уровняcompany.com. При этом оба дерева являются частями одного леса с общим "виртуальным" корнем.

При управлении деревьями и лесами нужно помнить два очень важных момента:

* первое созданное в лесу *доменов дерево* является *корневым деревом*, первый созданный в дереве домен называется *корневым доменом дерева* ( *tree root domain* );
* первый домен, созданный в лесу доменов, называется *корневым доменом леса* ( *forest root domain* ), данный домен не может быть удален (он хранит информацию о конфигурации леса и деревьях доменов, его образующих).

Организационные подразделения (ОП).

*Организационные подразделения*( *Organizational Units*, *OU* ) — контейнеры внутри AD, которые создаются для объединения объектов в целях *делегирования административных прав* и *применения групповых политик* в домене. ОП существуют *только внутри доменов* и могут объединять *только объекты из своего домена*. ОП могут быть вложенными друг в друга, что позволяет строить внутри домена сложную древовидную иерархию из контейнеров и осуществлять более гибкий административный контроль. Кроме того, ОП могут создаваться для отражения административной иерархии и организационной структуры компании.

**Глобальный каталог**

*Глобальный каталог* является перечнем *всех объектов*, которые существуют в лесу Active Directory. По умолчанию, контроллеры домена содержат только информацию об объектах своего домена. *Сервер Глобального каталога* является контроллером домена, в котором содержится информация о каждом объекте (хотя и не обо всех атрибутах этих объектов), находящемся в данном лесу.

**Именование объектов**

В службе каталогов должен быть механизм именования объектов, позволяющий однозначно идентифицировать любой объект каталога. В каталогах на базе протокола LDAP *для идентификации объекта в масштабе всего леса* используется механизм*отличительных имен* ( *Distinguished Name, DN* ). В Active Directory учетная запись пользователя с именем *User* доменаcompany.ru, размещенная в стандартном контейнере *Users*, будет иметь следующее отличительное имя: "DC=ru, DC=company, OU=Users, CN=User".

Обозначения:

* **DC** (Domain Component) — указатель на составную часть доменного имени;
* **OU** (Organizational Unit) — указатель на организационное подразделение (ОП);
* **CN** (Common Name) — указатель на общее имя.

Если отличительное имя однозначно определяет объект в масштабе всего леса, то для идентификации объекта относительно контейнера, в котором данный объект хранится, существует относительное отличительное имя ( *Relative Distinguished Name, RDN* ). Для пользователя *User* из предыдущего примера RDN-имя будет иметь вид " *CN=User* ".

Кроме имен DN и RDN, используется *основное имя* объекта ( *User Principal Name, UPN* ). Оно имеет формат <имя субъекта>@<суффикс домена>. Для того же пользователя из примера основное имя будет выглядеть как User@company.ru.

Имена DN, RDN могут меняться, если объект перемещается из одного контейнера AD в другой. Для того чтобы не терять ссылки на объекты при их перемещении в лесу, всем объектам назначается *глобально уникальный идентификатор* ( *Globally Unique Identifier, GUID* ), представляющий собой 128-битное число.

**Планирование пространства имен AD**

Планирование пространства имен и структуры AD — очень ответственный момент, от которого зависит эффективность функционирования будущей корпоративной системы безопасности. При этом надо иметь в виду, что созданную вначале структуру в процессе эксплуатации будет очень трудно изменить (например, в Windows 2000 изменить имя домена верхнего уровня вообще невозможно, а в Windows 2003 решение этой задачи требует выполнения жестких условий и тщательной подготовки данной операции). При планировании AD необходимо учитывать следующие моменты:

* тщательный выбор имен доменов верхнего уровня;
* качество коммуникаций в компании (связь между отдельными подразделениями и филиалами);
* организационная структура компании;
* количество пользователей и компьютеров в момент планирования;
* прогноз темпов роста количества пользователей и компьютеров.

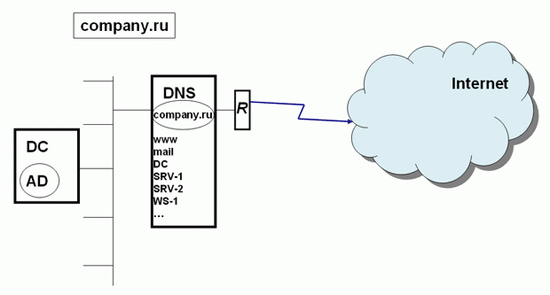
Рассмотрим вопрос пространства имен AD.

При планировании имен доменов верхнего уровня можно использовать различные стратегии и правила. В первую очередь необходимо учитывать вопросы интеграции внутреннего пространства имен и пространства имен сети Интернет — т.к. пространство имен AD базируется на пространстве имен DNS, при неправильном планировании могут возникнуть проблемы с безопасностью, а также конфликты с внешними именами.

Рассмотрим основные варианты.

1. Один домен, одна зона DNS (рис. 6.4).

На рисунке в левой части — внутренняя сеть компании, справа — сеть Интернет, две сети разделены маршрутизатором " *R* " (кроме маршрутизатора, на границе могут быть также прокси-сервер или межсетевой экран).

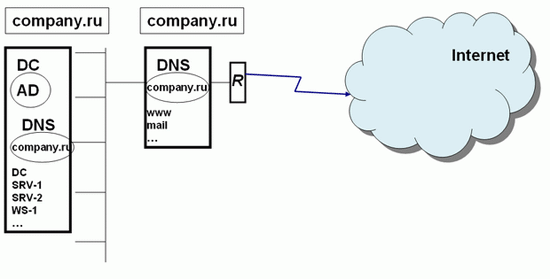


**Рис. 6.4.**

В данном примере используется одна и та же зона DNS (company.ru) как для поддержки внутреннего домена AD с тем же именем (записи DC, SRV-1, SRV-2, WS-1), так и хранения ссылок на внешние ресурсы компании — веб-сайт, почтовый сервер (записи www, mail ).

Такой способ максимально упрощает работу системного администратора, но при этом DNS-сервер, доступный для всей сети Интернет, хранит зону company.ru и предоставляет доступ к записям этой зоны всем пользователям Интернета. Таким образом, внешние злоумышленники могут получить полный список внутренних узлов корпоративной сети. Даже если сеть надежно защищена межсетевым экраном и другими средствами защиты, предоставление потенциальным взломщикам информации о структуре внутренней сети — вещь очень рискованная, поэтому данный способ организации пространства имен AD не рекомендуется (хотя на практике встречается довольно часто).

1. "Расщепление" пространства имен DNS - одно имя домена, две различные зоны DNS(рис. 6.5).

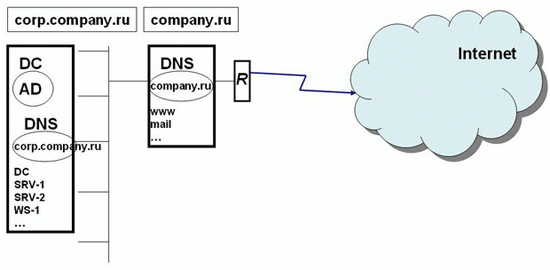


**Рис. 6.5.**

В данном случае на различных серверах DNS создаются различные зоны с одним и тем же именем company.ru. На внутреннем DNS-сервере функционирует зона company.ru.для Active Directory, на внешнем DNS-сервере — зона с таким же именем, но для ссылок на внешние ресурсы. Важный момент — данные зоны никак между собой не связаны — ни механизмами репликации, ни ручной синхронизацией.

Здесь во внешней зоне хранятся ссылки на внешние ресурсы, а во внутренней на внутренние ресурсы, используемые для работы Active Directory. Данный вариант несложно реализовать, но для сетевого администратора возникает нагрузка управления двумя разными доменами с одним именем.

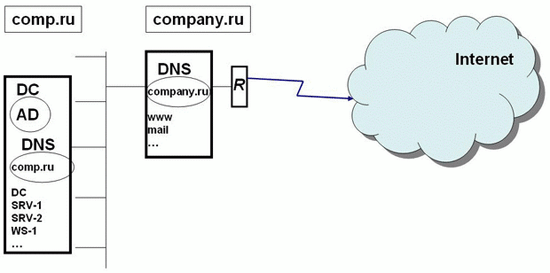
1. Поддомен в пространстве имен DNS для поддержки Active Directory (рис. 6.6).



**Рис. 6.6.**

В данном примере корневой домен компании company.ru служит для хранения ссылок на внешние ресурсы. В домене company.ru настраивается делегирование управление поддоменом corp.company.ru на внутренний DNS-сервер, и именно на базе домена corp.company.ru создается домен Active Directory. В этом случае во внешней зоне хранятся ссылки на внешние ресурсы, а также ссылка на делегирование управления поддоменом на внутренний DNS-сервер. Таким образом, пользователям Интернета доступен минимум информации о внутренней сети. Такой вариант организации пространства имен довольно часто используется компаниями.

1. Два различных домена DNS для внешних ресурсов и для Active Directory (рис. 6.7.).



**Рис. 6.7.**

В этом сценарии компания регистрирует в Интернет-органах два доменных имени: одно для публикации внешних ресурсов, другое — для развертывания Active Directory.

Данный сценарий планирования пространства имен самый оптимальный. Во-первых, имя внешнего домена никак не связано с именем внутреннего домена, и не возникает никаких проблем с возможностью показа в Интернет внутренней структуры. Во-вторых, регистрация (покупка) внутреннего имени гарантирует отсутствие потенциальных конфликтов, вызванных тем, что какая-то другая компания может зарегистрировать в Интернете имя, совпадающее с внутренним именем вашей компании.

1. Домен с именем типа company.local.

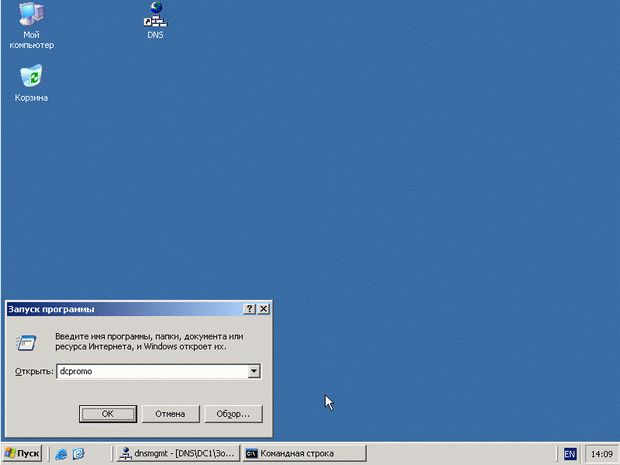
Во многих учебных пособиях и статьях используются примеры с доменными именами вида company.local. Такая схема вполне работоспособна и также часто применяется на практике. Однако в материалах разработчика системы Windows, корпорации Microsoft, нет прямых рекомендаций об использовании данного варианта.

**Установка контроллеров доменов**

Теперь перейдем к описанию процедур установки контроллеров доменов Active Directory.

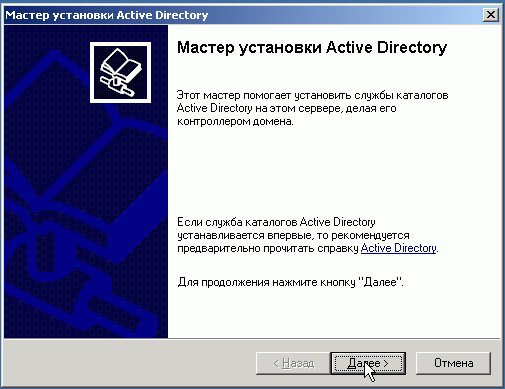
Разберем установку самого первого контроллера самого первого домена самого первого леса в структуре AD.

Установка начинается с запуска из командной строки мастера установки Active Directory — dcpromo (рис. 6.8).



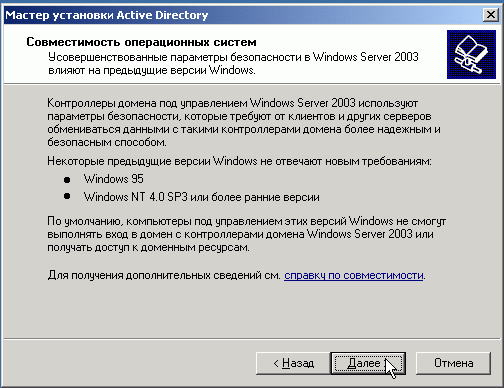
**Рис. 6.8.**

Нажимаем кнопку "ОК" и видим стартовую страницу мастера (рис. 6.9):



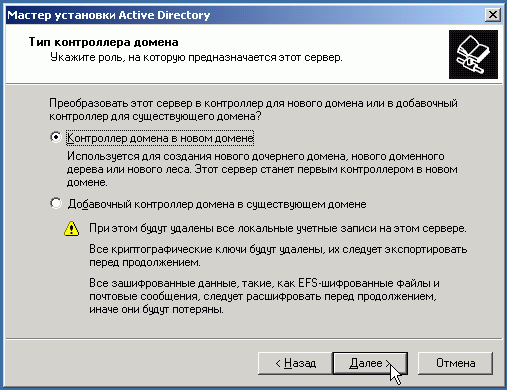
**Рис. 6.9.**

Далее идет предупреждение, что операционные системы Windows 95, Windows NT 4.0 SP3 и более ранние не смогут функционировать в доменах Windows 2003 (рис. 6.10). Заметим, что в доменах на базе Windows 2000 такой проблемы нет (да и в доменах на базе windows 2003 эта проблема решаема).

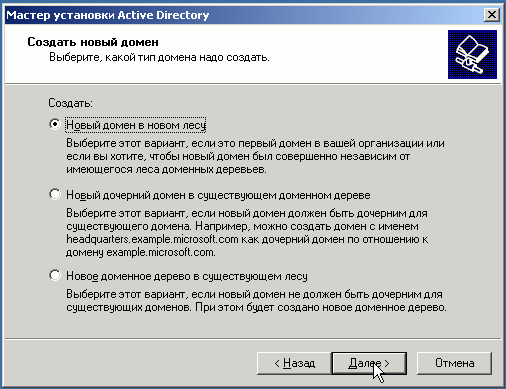


**Рис. 6.10.**

Затем выбираем варианты установки контроллера домена в новом домене (рис. 6.11) и создания нового домена в новом лесу (рис. 6.12):

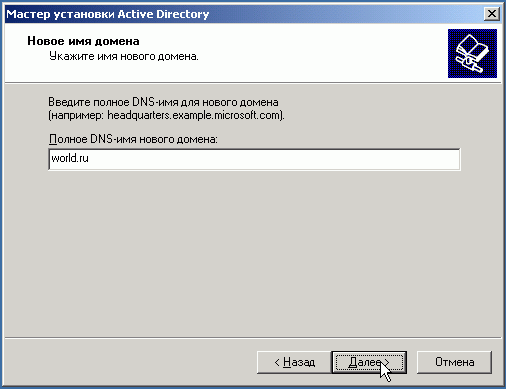


**Рис. 6.11.**



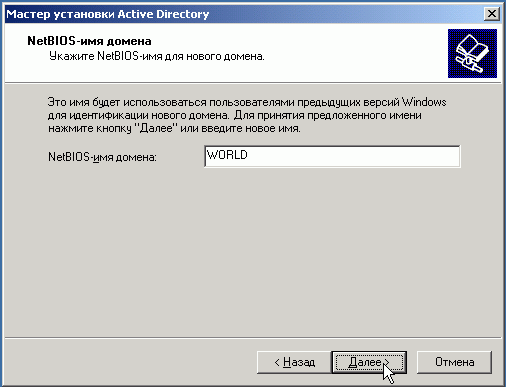
**Рис. 6.12.**

Следующий шаг — выбор имени домена (для Active Directory это будет корневой домен). В нашем примере выберем имя world.ru (рис. 6.13):



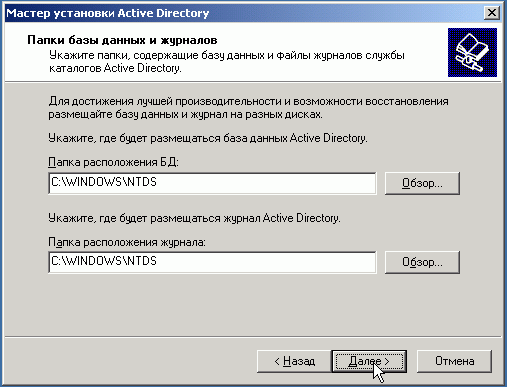
**Рис. 6.13.**

Зададим NetBIOS-имя домена (по умолчанию, будет предложена левая часть полного имени домена, выбранного на предыдущем шаге). В нашем примере — WORLD (рис. 6.14.):

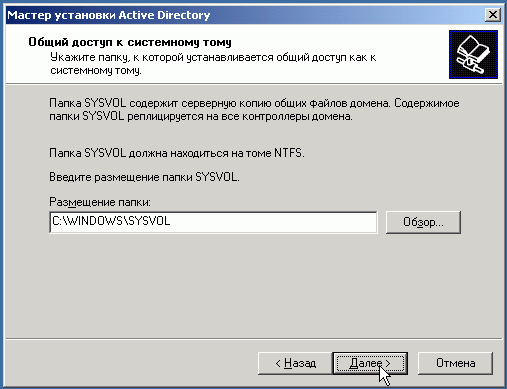


**Рис. 6.14.**

Далее мастер предложит выбрать место на жестких дисках для размещения базы данных Active Directory, журнала транзакций этой БД (рис. 6.15) и папки системного тома SYSVOL (рис. 6.16). Системный том обязательно должен быть размещен на разделе с файловой системой NTFS.

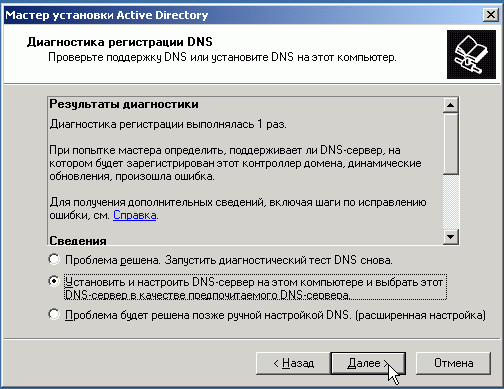


**Рис. 6.15.**



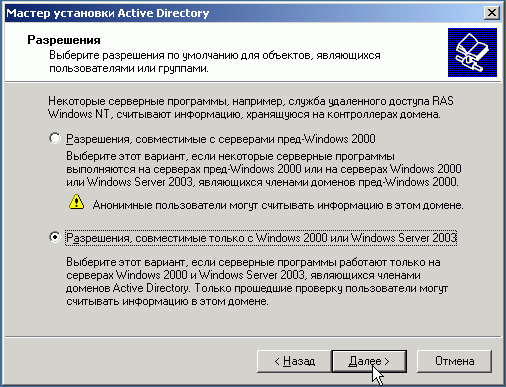
**Рис. 6.16.**

После этого мастер установки на основе параметров сетевой конфигурации сервера ищет в сети DNS-сервер, на котором имеется зона с указанным нами именем домена, причем в данной зоне должны быть разрешены динамические обновления. Если такой сервер DNS в сети не найден, то мастер предложит установить службу DNS на данном сервере и создать соответствующую зону (рис. 6.17):



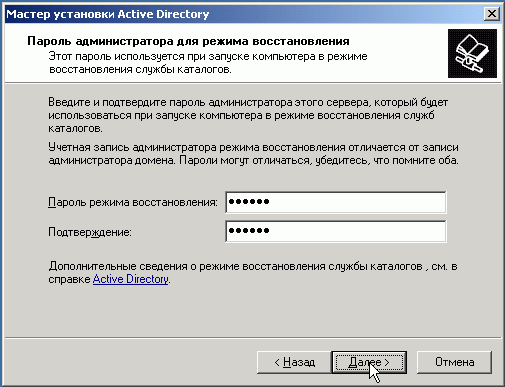
**Рис. 6.17.**

Далее предлагается выбрать уровень разрешений создаваемого домена (рис. 6.18). Заметим, что если мы выберем наиболее высокий уровень, то в таком домене не смогут существовать компьютеры с операционными системами, более ранними, чем Windows 2000.



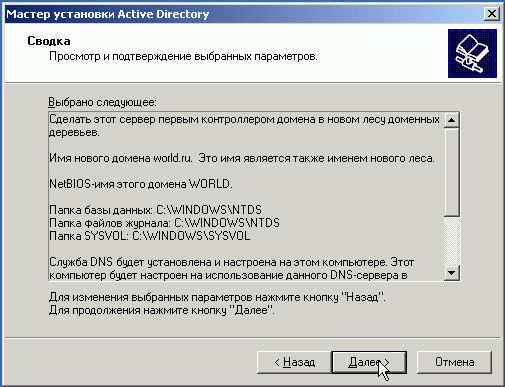
**Рис. 6.18.**

Затем задаем пароль администратора при запуске системы в режиме восстановления служб каталогов (рис. 6.19). данный режим используется для восстановления БД Active Directory из резервной копии.



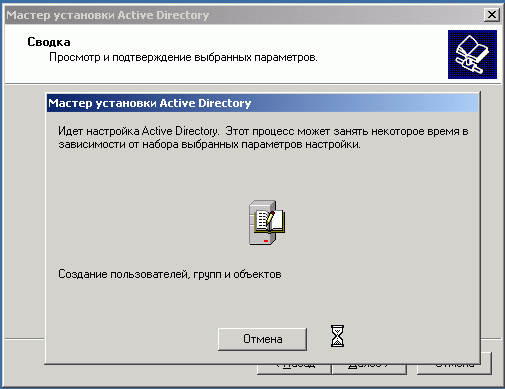
**Рис. 6.19.**

Затем следует экран со сводкой информации о создаваемом домене и параметрах контроллера домена (рис. 6.20). На этом шаге в случае обнаруженной ошибки в конфигурации можно вернуться назад и исправить ошибку.



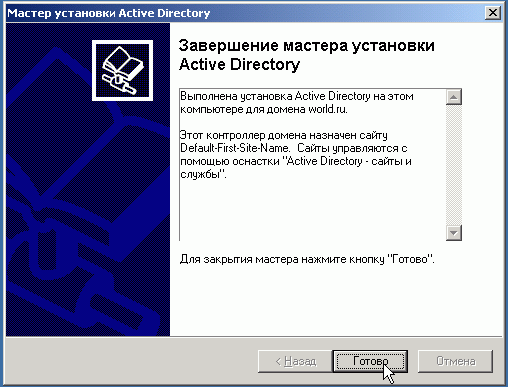
**Рис. 6.20.**

После этого начинается работа по созданию базы данных AD и наполнению ее нужными записями (рис. 6.21).



**Рис. 6.21.**

Последний шаг — нажать кнопку "Готово" и перезагрузить сервер (рис. 6.22).

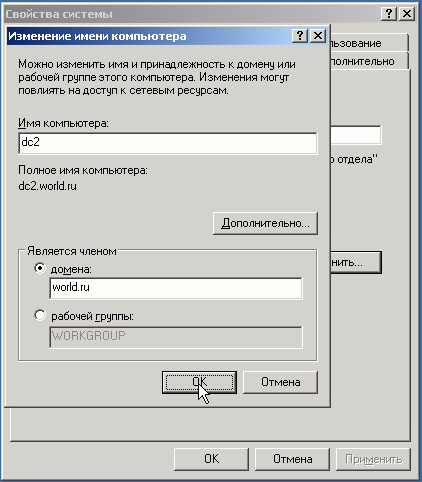


**Рис. 6.22.**

**Важное замечание**. Если при создании первого контроллера в домене перед запуском мастера в локальной базе SAM данного сервера были какие-либо учетные записи пользователей и групп, то все они импортируются в созданную БД Active Directory с сохранением своих имен и паролей, в том числе и учетная запись администратора сервера, которая становится учетной записью администратора домена (а если самый первый домен в лесу, то и администратором предприятия и администратором схемы).

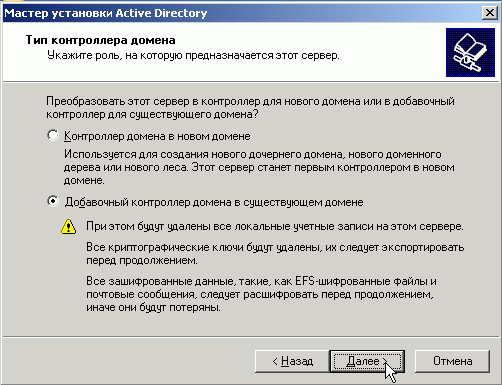
Кратко опишем процесс установки дополнительного контроллера в уже созданном домене.

Если у нас есть второй сервер, который мы хотим сделать дополнительным контроллером домена, то вначале желательно включить его в домен в качестве сервера–члена домена. Кнопка "Пуск" — Панель управления — Система — Закладка "Имя компьютера" — Кнопка "Изменить". Далее в поле "Является членом домена" ввести имя домена, нажать ОК, ввести имя и пароль администратора домена, снова нажать ОК и перезагрузить сервер (рис. 6.23).



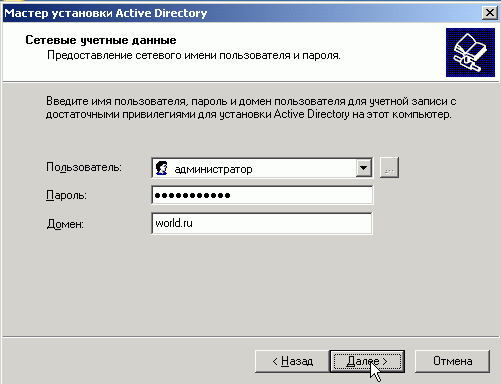
**Рис. 6.23.**

После перезагрузки входим в систему с учетной записью администратора домена и запускаем мастер установки Active Directory — команда dcpromo. Выбираем вариант "Добавочный контроллер в существующем домене" (рис. 6.24).



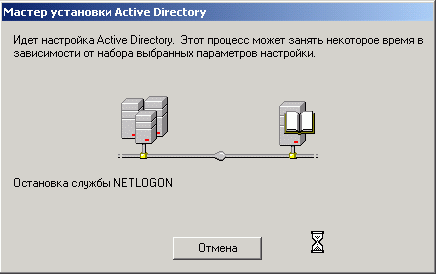
**Рис. 6.24.**

Указываем учетные данные администратора домена (рис. 6.25):



**Рис. 6.25.**

Снова указываем имя домена — world.ru. Начинается процесс импорта БД Active Directory на создаваемый контроллер (рис. 6.26):



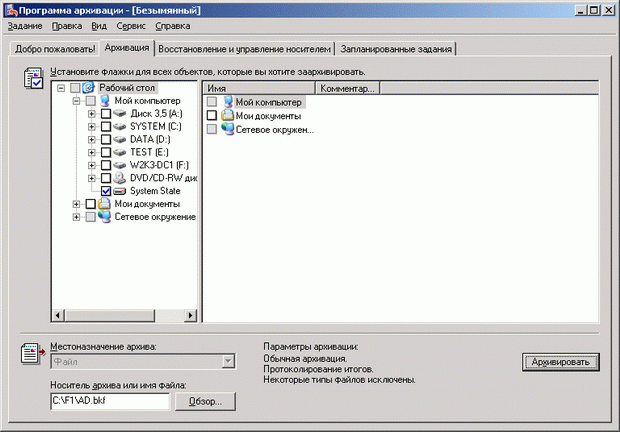
**Рис. 6.26.**

По окончании процесса — снова нажать кнопку "Готово" и перезагрузить сервер.

**Важное замечание**. При добавлении дополнительного контроллера в домене существовавшая на сервере локальная база SAM с сервера удаляется.

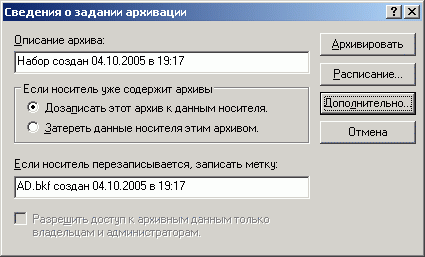
Опишем процесс установки дополнительного контроллера домена из резервной копии AD существующего контроллера.

Сначала создадим резервную копию AD. Запустим на существующем контроллере домена утилиту ntbackup, выберем архивацию состояния системы (System State), укажем путь для создания файла с резервной копией и нажмем кнопку "Архивировать" (рис. 6.27):



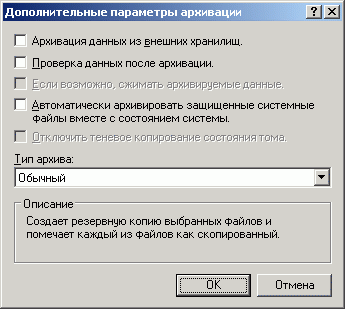
**Рис. 6.27.**

На следующем шаге — нажать кнопку "Дополнительно" (рис. 6.28):



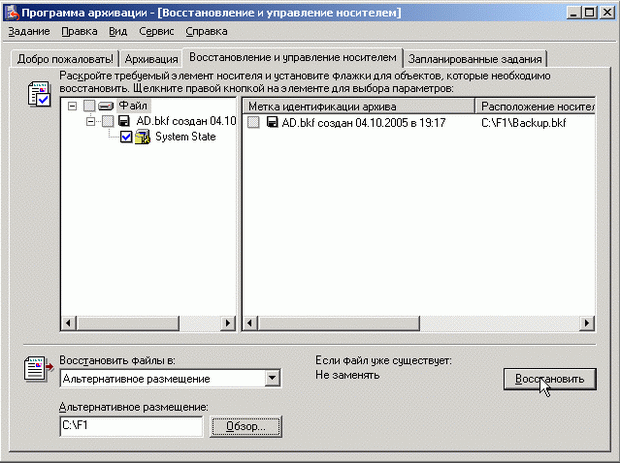
**Рис. 6.28.**

В открывшейся панели — убрать галочку у поля "Автоматически архивировать защищенные системные файлы вместе с состоянием системы" (рис. 6.29):



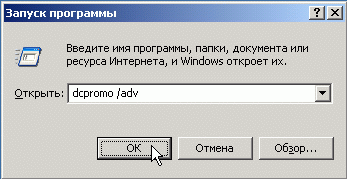
**Рис. 6.29.**

После создания резервной копии AD файл с резервной копией желательно скопировать на жесткий диск того сервера, который будет преобразовываться в контроллер домена. Затем надо разархивировать резервную копию утилитой ntbackup. При этом обязательно надо указать, что восстанавливать данные надо в альтернативное размещение и указать папку для размещения восстановленных данных (рис. 6.30):



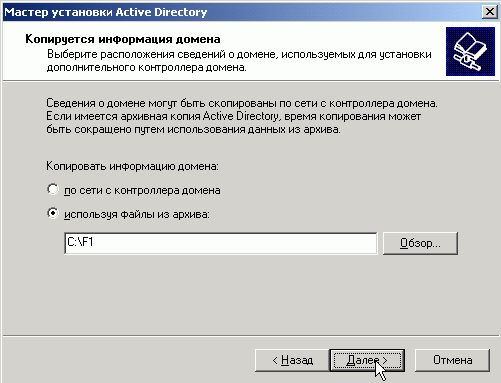
**Рис. 6.30.**

Теперь на сервере, который преобразуем из простого сервера в контроллер домена, запускаем утилиту dcpromo с параметром "/adv" (рис. 6.31):



**Рис. 6.31.**

На этапе выбора источника БД Active Directory — выбрать вариант "используя файлы из архива" и указать путь к папке, в которую разархивировали резервную копию (рис. 6.32):



**Рис. 6.32.**

По окончании процесса — перезагрузить сервер.

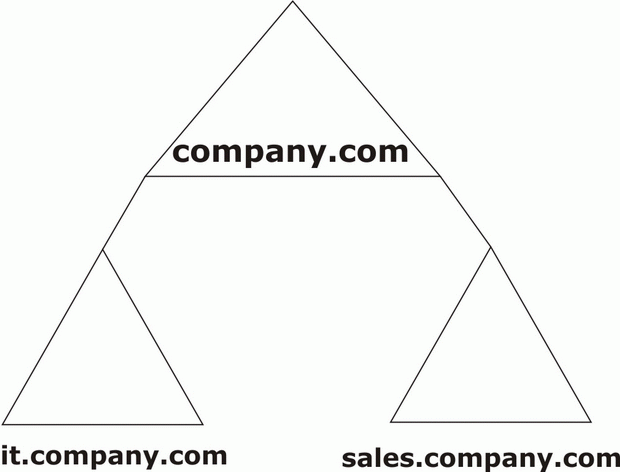
**6.2 Логическая и физическая структуры, управление репликацией AD. Серверы Глобального каталога и Хозяева операций**

**Логическая структура Active Directory**

Служба каталогов Active Directory организована в виде иерархической структуры, построенной из различных компонентов, которые представляют элементы корпоративной сети. В этой структуре есть, например, *пользовательские объекты*, компьютерные объекты, и различные контейнеры. Способ организации этих элементов представляет собой логическую структуру Active Directory в корпоративной сети. Логическая структура Active Directory включает в себя леса, деревья, домены и Организационные подразделения (ОП). Каждый из элементов логической структуры описан ниже.

**Домен** — логическая группа пользователей и компьютеров, которая поддерживает централизованное администрирование и управление безопасностью. Домен является единицей безопасности – это означает, что администратор для одного домена, по умолчанию, не может управлять другим доменом. Домен также является основной единицей для репликации — все контроллеры одного домена должны участвовать в репликации друг с другом. Домены в одном лесу имеют автоматически настроенные доверительные отношения, что позволяет пользователям из одного домена получать доступ к ресурсам в другом. Необходимо также знать, что можно создавать доверительные отношения с внешними доменами, не входящими в лес.

**Дерево** является набором доменов, которые связаны отношениями "дочерний"/"родительский", а также используют связанные (смежные, или прилегающие) пространства имен. При этом дочерний домен получает имя от родительского. Например, можно создать дочерний домен, называемый it, в домене company.com, тогда его полное имя будет it.company.com (рис. 6.33). Между доменами автоматически устанавливаются двухсторонние транзитивные доверительные отношения (домен it.company.com доверяет своему "родительскому" домену, который в свою очередь "доверяет" домену sales.company.com – таким образом, доменit.company.com доверяет домену sales.company.com, и наоборот). Это означает, что доверительные отношения могут быть использованы всеми другими доменами данного леса для доступа к ресурсам данного домена. Заметим, что домен it.company.com продолжает оставаться самостоятельным доменом, в том смысле, что он остается единицей для управления системой безопасности и процессом репликации. Поэтому, например, администраторы из домена sales.company.com не могут администрировать домен it.company.com до тех пор, пока им явно не будет дано такое право.



**Рис. 6.33.**

**Лес** — это одно или несколько деревьев, которые разделяют общую *схему*, серверы *Глобального каталога* и *конфигурационную информацию*. В лесу все домены объединены транзитивными двухсторонними доверительными отношениями.

Каждая конкретная инсталляция Active Directory является *лесом*, даже если состоит всего из одного домена.

**Организационное подразделение (ОП)** является контейнером, который помогает группировать объекты для целей администрирования или применения групповых политик. ОП могут быть созданы для организации объектов в соответствии с их функциями, местоположением, ресурсами и так далее. Примером объектов, которые могут быть объединены в ОП, могут служить учетные записи пользователей, компьютеров, групп и т.д. Напомним, что ОП может содержать только объекты из того домена, в котором они расположены.

Подводя итог, можно сказать, что *логическая структура* Active Directory позволяет организовать ресурсы корпоративной сети таким образом, чтобы они отражали структуру самой компании.

#### Физическая структура Active Directory

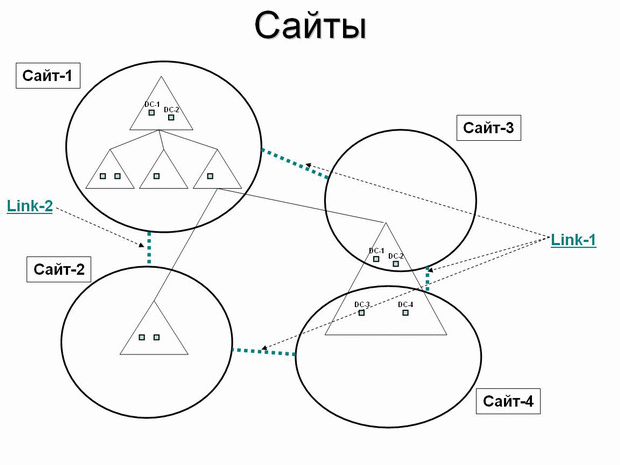
Физическая структура Active Directory служит для связи между логической структурой AD и *топологией* корпоративной сети.

Основные элементы физической структуры Active Directory — *контроллеры домена* и *сайты*.

Контроллеры домена были подробно описаны в предыдущем разделе.

**Сайт** — группа IP-сетей, соединенных быстрыми и надежными коммуникациями. Назначение сайтов — управление процессом репликации между контроллерами доменов и процессом аутентификации пользователей. Понятие "быстрые коммуникации" очень относительное, оно зависит не только от качества линий связи, но и от объема данных, передаваемых по этим линиям. Считается, что быстрый канал — это не менее 128 Кбит/с (хотя Microsoft рекомендует считать быстрыми каналы с пропускной способностью не менее 512 Кбит/с).

Структура сайтов никак не зависит от структуры доменов. Один домен может быть размещен в нескольких сайтах, и в одном сайте могут находиться несколько доменов (рис. 6.34).



**Рис. 6.34.**

Поскольку сайты соединяются друг с другом медленными линиями связи, механизмы репликации изменений в AD внутри сайта и между сайтами различные. Внутри сайта контроллеры домена соединены линиями с высокой пропускной способностью. Поэтому репликация между контроллерами производится каждые 5 минут, данные при передаче не сжимаются, для взаимодействия между серверами используется технология вызова удаленных процедур (RPC). Для репликации между сайтами кроме RPC может использоваться также протокол SMTP, данные при передаче сжимаются (в результате сетевой трафик составляет от 10 до 40% от первоначального значения), передача изменений происходит по определенному расписанию. Если имеется несколько маршрутов передачи данных, то система выбирает маршрут с наименьшей стоимостью.

Кроме управления репликацией, сайты используются при аутентификации пользователей в домене. Процесс аутентификации может вызвать заметный трафик, особенно если в сети имеется большое количество пользователей (особенно в начале рабочего дня, когда пользователи включают компьютеры и регистрируются в домене). При входе пользователя в сеть его аутентификация осуществляется *ближайшим контроллером домена*. В процессе поиска "ближайшего" контроллера в первую очередь используется информация о сайте, к которому принадлежит компьютер, на котором регистрируется пользователь. Ближайшим считается контроллер, расположенный в том же сайте, что и регистрирующийся пользователь. Поэтому рекомендуется в каждом сайте установить как минимум один контроллер домена.

В процессе аутентификации большую роль играет также *сервер глобального каталога* (при использовании универсальных групп). Поэтому в каждом сайте необходимо также размещать как минимум один *сервер глобального каталога* (или на одном из контроллеров домена в каждом сайте настроить кэширование членства в универсальных группах). Пользователи сети (в том числе компьютеры и сетевые службы) используют *серверы глобального каталога* для поиска объектов. В случае, если доступ к серверу глобального каталога осуществляется через линии связи с низкой пропускной способностью, многие операции службы каталога будут выполняться медленно. Это обстоятельство также стимулирует установку *сервера глобального каталога* в каждом сайте (более подробно о*серверах глобального каталога* будет рассказано ниже).

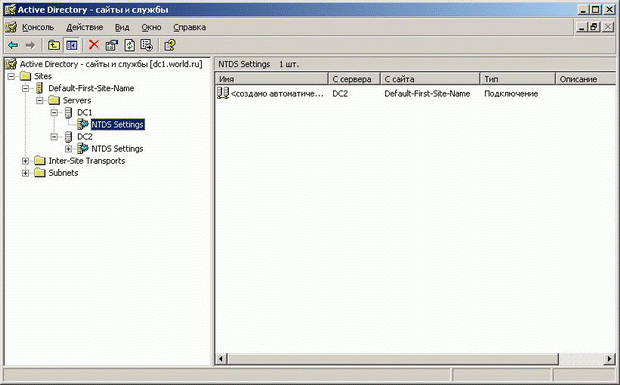
В самом начале создания леса автоматически создается сайт по умолчанию с именем *Default-First-site-Name*. В дальнейшем сетевой администратор должен сам планировать и создавать новые сайты и определять входящие в них подсети, а также перемещать в сайты соответствующие контроллеры доменов. При создания*нового* контроллера на основании выделенного ему IP-адреса служба каталога *автоматически* отнесет его к соответствующему сайту.

#### Репликация, управление топологией репликации

Рассмотрим сам процесс репликации изменений в AD как внутри сайта, так и между сайтами.

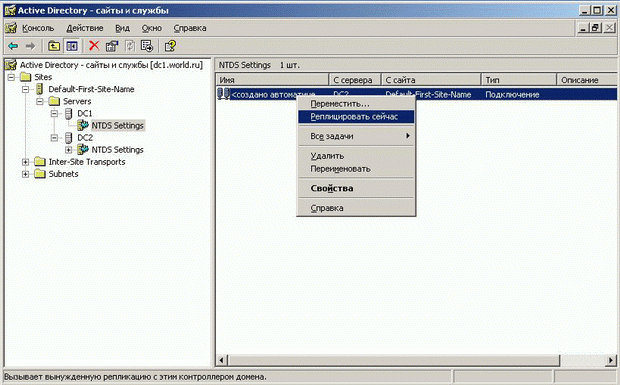
##### Репликация внутри сайта

Репликация изменений в AD между контроллерами домена происходит автоматически, каждые 5 минут. Топологию репликации, т.е. порядок, в котором серверы опрашивают друг друга для получения изменений в базе данных, серверы строят автоматически (эту задачу выполняет компонента служб каталогов, называемая*Knowledge Consistency Checker*, или *KCC*, вариант перевода данного термина — " *наблюдатель показаний целостности* "). При достаточно большом количестве контроллеров KCC строит кольцевую топологию репликации, причем для надежности образует несколько колец, по которым контроллеры передают данные репликации. Наглядно увидеть топологию репликации можно с помощью административной консоли " *Active Directory - сайты и службы* ". Если в этой консоли раскрыть последовательно контейнеры *Sites*, *Defauit-First-site-Name*, *Servers*, далее — конкретный сервер (например, DC1) и установить на узле *NTDS Settings*, то в правой половине окна видно, что сервер DC1 запрашивает изменения с сервера DC2 (рис. 6.35):



**Рис. 6.35.**

Возможностей управления репликацией у администратора сети в данном случае немного. Можно лишь вызвать принудительную репликацию в той же консоли "*Active Directory - сайты и службы* ". Если в правой части того же окна консоли, изображенного на рис. 6.35, щелкнуть правой кнопкой мыши на имени DC2 и выбрать вариант " *Реплицировать сейчас* ", то контроллер DC1 получит изменения в базе данных AD с контроллера DC2 (рис. 6.36):



**Рис. 6.36.**

##### Репликация между сайтами

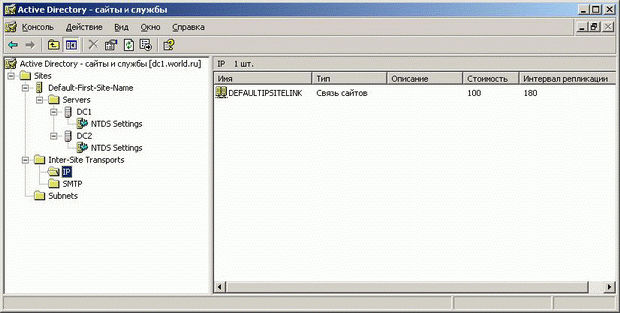
Разбивать большую корпоративную сеть на отдельные сайты необходимо по следующим причинам: отдельные подсети корпоративной сети, расположенные в удаленных офисах, могут быть подключены друг к другу медленными каналами связи, которые сильно загружены в течение рабочего дня; поэтому возникает необходимость осуществления репликации в те часы, когда сетевой трафик минимален, и передавать данные репликации со сжатием.

Вернемся к сетевой структуре, изображенной на рис. 6.34, и обсудим понятия и термины, играющие важную роль в управлении репликацией между сайтами.

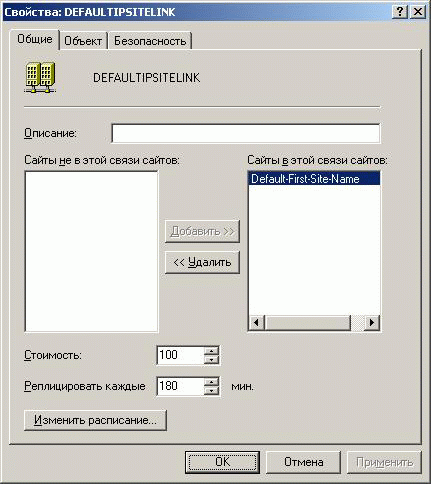
В этой конфигурации топология репликации также строится системной компонентой *KCC*. KCC выбирает контроллеры, которые осуществляют репликацию между сайтами, проверяет их работоспособность и, в случае недоступности какого-либо сервера, назначает для репликации другой доступный сервер.

Для репликации между сайтами используется тот или иной *межсайтовый транспорт* — это либо *IP* ( *RPC* ), либо *SMTP*. Для каждого вида межсайтового транспорта определяется " *соединение сайтов* " ( *site link* ), с помощью которого строится управление репликацией между двумя и более сайтами. Именно для соединения ("линка") задаются такие параметры как " *Расписание репликации* " и " *Стоимость* ". На рис. 6.34. соединение *Link-1* связывает в единую цепочку сайты *Сайт-1*,*Сайт-3*, *Сайт-4* и *Сайт-2*, соединение *Link-2* связывает два сайта — *Сайт-1* и *Сайт-2*. В данном примере репликация между сайтами *Сайт-1* и *Сайт-2* будет проходить либо по соединению *Link-1*, либо по соединению *Link-2* — в зависимости от расписания, стоимости соединения и его доступности (при доступности обоих соединений преимущество будет иметь соединение с более низкой стоимостью). На рис. 6.37 изображено созданное автоматически соединение для транспорта *IP* (*RPC* ) — *DEFAULTIPSITELINK*. Если открыть *Свойства* этого соединения (рис. 6.38), то можно управлять списком сайтов, относящихся к этому соединению, назначать стоимость соединения (значение по умолчанию — 100), интервал репликации (по умолчанию — каждые 3 часа), а если нажать кнопку " *Изменить расписание* ", то можно более тонко определить дни и часы, в которые будет производиться репликация.

Контейнер *Subnets* консоли " *Active Directory - сайты и службы* " служит для описания подсетей, входящих в тот или иной сайт.



**Рис. 6.37.**



#### Рис. 6.38. Функциональные уровни домена и леса

Набор возможностей, предоставляемых службой каталогов Active Directory, зависит от того, на каком уровне (или в каком режиме) функционируют отдельный домен или весь лес в целом.

Для Windows 2003 имеются 4 уровня функционирования (в Windows 2000 — 2 уровня):

*Windows 2000 смешанный (Windows 2000 mixed)*

В данном режиме в домене могут существовать резервные контроллеры домена под управлением системы Windows NT Server. Этот режим рассматривается как переходный в процессе модернизации служб каталогов с Windows NT на Windows 2000/2003. В этом режиме отсутствует ряд возможностей Active Directory — универсальные группы, вложенность групп. Кроме того, наличие контроллеров домена под управлением Windows NT накладывает ограничение на размер БД Active Directory (40 мегабайт).

После установки системы и создания первого контроллера домена домен всегда работает именно в смешанном режиме.

*Windows 2000 основной (Windows 2000 native)*

В данном режиме контроллерами домена могут быть серверы под управлением Windows 2000 и Windows 2003. В данном режиме появляется возможность использования универсальных групп, вложенность групп, и ликвидируется ограничение на размер БД Active Directory.

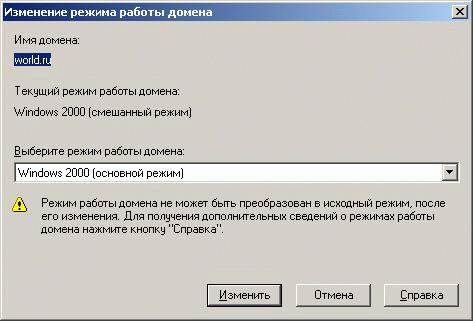
*Windows 2003 промежуточный (Windows 2003 interim)*

Данный уровень возможен только в том случае, когда контроллеры домена работают под управлением Windows NT и Windows 2003 (не может быть контроллеров с системой Windows 2000). Этот уровень доступен только тогда, когда производится установка Windows 2003 поверх контроллеров домена с Windows NT. Ограничения этого режима аналогичны смешанному режиму.

*Windows 2003*

Это наивысший уровень функционирования домена, в котором есть контроллеры с Windows 2003, причем все контроллеры обязаны быть с системой Windows 2003.

Изменять уровень функционирования домена можно *только в сторону его повышения*. Сделать это можно с помощью административных консолей " *Active Directory – домены и доверие* " или " *Active Directory – пользователи и компьютеры* ". Если в какой-либо из этих консолей щелкнуть правой кнопкой мыши на имени домена и выбрать в контекстном меню пункт " *Изменение режима работы домена* ", то появится панель, изображенная на рис. 6.39:



**Рис. 6.39.**

Для повышения уровня надо выбрать необходимый уровень и нажать кнопку " *Изменить* ". После репликации данного изменения на все контроллеры в данном домене станут доступны специфичные для данного уровня возможности. Заметим, что произведенные изменения необратимы.

Для всего леса в целом также можно определять функциональные уровни. Это делается с помощью консоли " *Active Directory – домены и доверие* ". Только правой кнопкой мыши надо щелкнуть не на имени домена, а на надписи " *Active Directory – домены и доверие* ".

Существуют 3 уровня функционирования леса:

* Windows 2000 (с контроллерами под управлением Windows NT, 2000 и 2003);
* Windows 2003 interim (с контроллерами под управлением только Windows NT и 2003);
* Windows 2003 ( *все домены всего леса* — с контроллерами под управлением *только* Windows 2003).

Самый высокий уровень функционирования леса позволяет выполнять две очень важные задачи:

* переименование доменов;
* установление доверительных отношений между двумя *не связанными друг с другом* лесами с использованием Kerberos в качестве протокола аутентификации (без такого режима доверительные отношения могут устанавливаться только между отдельными доменами, а не целыми лесами, при этом будет использоваться менее защищенный протокол аутентификации *NTLM*).

#### Серверы Глобального каталога и Хозяева операций

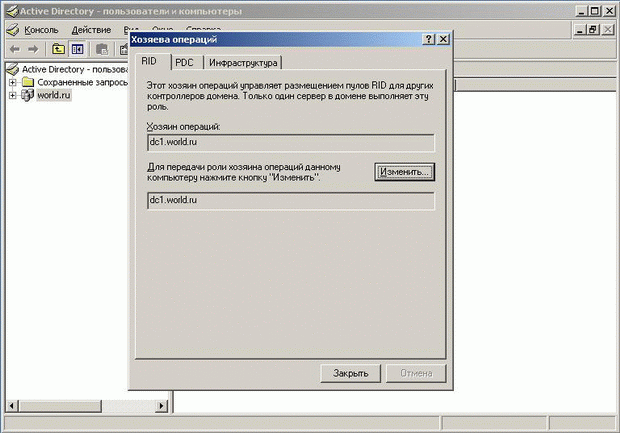
Большинство операций с записями БД Active Directory администратор может выполнять, подключившись с помощью соответствующей консоли к любому из контроллеров домена. Однако, во избежание несогласованности, некоторые действия должны быть скоординированы и выполнены специально выделенными для данной цели серверами. Такие контроллеры домена называются *Хозяевами операций* ( *Operations Masters* ), или *исполнителями специализированных ролей* (*Flexible Single-Master Operations*, сокращенно — *FSMO* ).

Всего имеется пять специализированных ролей:

1. **Schema Master (хозяин схемы)**: контролирует возникающие изменения Схемы базы данных Active Directory (добавление и удаление классов объектов, модификация набора атрибутов). *Один* контроллер домена *в масштабе всего леса* выполняет эту роль (по умолчанию — самый первый контроллер в лесу).
2. **Domain Naming Master (хозяин именования доменов)**: контролирует процесс добавления или удаления доменов в лесу. *Один* контроллер домена *в масштабе всего леса* выполняет эту роль (по умолчанию — самый первый контроллер в лесу).
3. **PDC Emulator (эмулятор PDC)**: действует как PDC (главный контроллер домена) для *BDC* (резервный контроллер домена) под управлением Windows NT, когда домен находится в смешанном режиме; управляет изменениями паролей (изменение пароля учетной записи в первую очередь реплицируется на эмулятор PDC); является предпочтительным сервером (в Windows 2000 — единственный сервер) для редактирования групповых политик; является сервером времени для остальных контроллеров данного домена (контроллеры домена синхронизируют свои системные часы с эмулятором PDC). *Один* контроллер *в домене* выполняет эту роль (по умолчанию — самый первый контроллер в домене).
4. **RID Master (хозяин RID, распределитель идентификаторов учетных записей)**: выделяет контроллерам домена пулы относительных идентификаторов (RID, которые являются уникальной частью идентификаторов безопасности SID). *Один* контроллер *в домене* выполняет эту роль (по умолчанию — самый первый контроллер в домене).
5. **Infrastructure Master (хозяин инфраструктуры)**: отвечает за обновление связей "пользователи — группы" между доменами. Эта роль не должна храниться на контроллере домена, который также является *сервером Глобального Каталога* – *хозяин инфраструктуры* не будет работать в данном сценарии (за исключением случая, когда в домене всего один контроллер). *Один* контроллер *в домене* выполняет эту роль (по умолчанию — самый первый контроллер в домене).

Просмотреть текущих владельцев ролей и передать ту или иную роль на другой контролер можно с помощью административных консолей:

* роль *Хозяина Схемы* — с помощью консоли " *Active Directory Schema* " (чтобы запустить эту консоль, надо сначала зарегистрировать соответствующую программную компоненту в командной строке: regsvr32 schmmgmt.dll, а затем запустить саму консоль тоже в командной строке — schmmgmt.msc );
* роль *Хозяина именования доменов* — с помощью консоли " *Active Directory – домены и доверие* ";
* роли *эмулятора PDC*, *хозяина RID* и *хозяина инфраструктуры* — с помощью консоли " *Active Directory – пользователи и компьютеры* " (пример можно увидеть нарис. 6.40).



**Рис. 6.40.**

Необходимо знать, кто из пользователей имеет право менять роли хозяев операций:

* эмулятор PDC — члены группы " *Администраторы домена* ";
* *хозяин RID* — члены группы " *Администраторы домена* ";
* *хозяин инфраструктуры* — члены группы " *Администраторы домена* ";
* *хозяин именования доменов* — члены группы " *Администраторы предприятия* ";
* *хозяин схемы* — члены группы " *Администраторы Схемы* " или группы " *Администратор предприятия* ".

Если контроллер домена, которому принадлежит роль хозяина операции, выходит из строя (вследствие *повреждения оборудования* или программного обеспечения), причем нет возможности восстановить данную систему из резервной копии, то с помощью административных консолей передать роли работоспособным серверам нет возможности. Восстановить функционирование определенной роли хозяина операций можно только путем захвата данной роли с помощью утилиты командной строки ntdsutil.

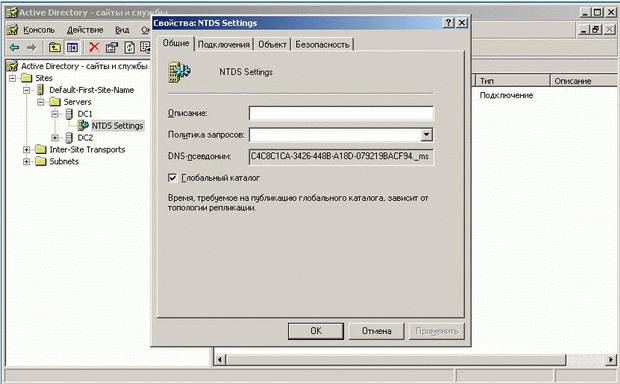
##### Сервер глобального каталога

Напомним, что *Глобальный каталог* ( *global catalog* ) — это перечень *всех объектов* леса Active Directory. По умолчанию, контроллеры домена содержат только информацию об объектах своего домена. *Сервер Глобального каталога* является контроллером домена, в котором содержится информация *о каждом объекте* (хотя и не обо всех атрибутах этих объектов), находящемся в данном лесу.

*Сервер глобального каталога* выполняет две очень важные функции:

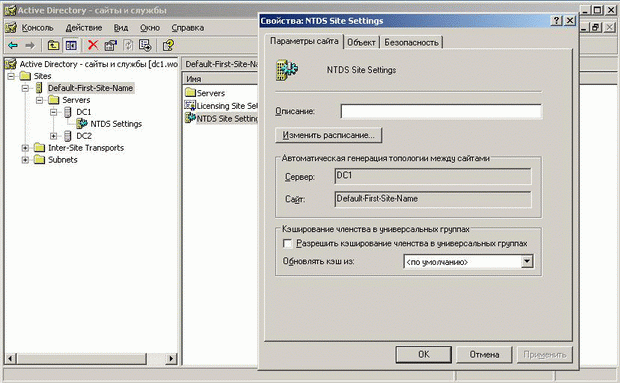
* поиск объектов в масштабах всего леса (клиенты могут обращаться к глобальному каталогу с запросами на поиск объектов по определенным значениям атрибутов; использование *сервера глобального каталога* — единственный способ осуществлять поиск объектов по всему лесу);
* аутентификация пользователей (*сервер глобального каталога* предоставляет информацию о членстве пользователя в *универсальных группах*, *universal groups* ; поскольку универсальные группы со списками входящих в них пользователей хранятся только на *серверах глобального каталога*, аутентификация пользователей, входящих в такие группы, возможна только при участии *сервера глобального каталога*).

По умолчанию самый первый контроллер домена в лесу является *сервером глобального каталога*. Однако администратор сети может назначить любой контроллер домена *сервером глобального каталога*. Это делается с помощью административной консоли " *Active Directory – сайты и службы* ", в свойствах узла " *NTDS Settings*" выбранного контроллера (рис. 6.41):



**Рис. 6.41.**

Для эффективной работы службы каталогов Active Directory необходимо, чтобы в каждом сайте AD был либо *сервер глобального каталога*, либо контроллер домена, кэширующий у себя списки членов универсальных групп. Кэширование универсальных групп также настраивается в консоли " *Active Directory – сайты и службы* " в свойствах узла " *NTDS Settings* " для каждого сайта Active Directory. Для включения кэширования нужно поставить галочку у поля " *Разрешить кэширование членства в универсальных группах* " и указать, из какого сайта данный сайт будет получать списки универсальных групп в поле " *Обновлять кэш из*:" (рис. 6.42):



**Рис. 6.42.**

### 6.3 Управление пользователями и группами. Управление организационными подразделениями, делегирование полномочий. Групповые политики

#### Управление пользователями и группами

*Учетные записи* ( *accounts* ) пользователей, компьютеров и групп — один из главных элементов управления доступом к сетевым ресурсам, а значит, и всей системы безопасности сети в целом.

В среде Windows 2003 Active Directory существует 3 главных типа пользовательских учетных записей:

* **Локальные учетные записи пользователей**. Эти учетные записи существуют в локальной базе данных *SAM* ( *Security Accounts Manager* ) на каждой системе, работающей под управлением Windows 2003. Эти учетные записи создаются с использованием инструмента *Local Users and Groups* ( *Локальные пользователи и группы* ) консоли *Computer Management*( *Управление компьютером* ). Заметим, что для входа в систему по локальной учетной записи, эта учетная запись обязательно должна присутствовать в базе данных SAM на системе, в которую вы пытаетесь войти. Это делает локальные учетные записи непрактичными для больших сетей, вследствие больших накладных расходов по их администрированию.
* **Учетные записи пользователей домена**. Эти учетные записи хранятся в Active Directory и могут использоваться для входа в систему и доступа к ресурсам по всему лесу AD. Учетные записи этого типа создаются централизованно при помощи консоли " *Active Directory Users and Computers* " (" *Active Directory – пользователи и компьютеры* ").
* **Встроенные учетные записи**. Эти учетные записи создаются самой системой и не могут быть удалены. По умолчанию любая система, будь то изолированная (отдельно стоящая) или входящая в домен, создает две учетные записи –*Administrator* ( *Администратор* ) и *Guest* ( *Гость* ). По умолчанию учетная запись Гость отключена.

Сосредоточим свое внимание на учетных записях пользователей домена. Эти учетные записи хранятся на контроллерах домена, хранящих копию базы данных Active Directory.

Существуют различные форматы, в которых могут быть представлены имена для входа пользователей в систему, потому что они могут отличаться для целей совместимости с клиентами, работающими под управлением более ранних версий Windows (такими как 95, 98, NT). Два основных вида имен входа — это с использованием суффикса *User Principal Name* ( *основного имени пользователя* ) и имя входа пользователя в системах пред-Windows 2000.

Основное имя пользователя ( *UPN*, *User Principle Name* ) имеет такой же формат, как и электронный адрес. Он включает в себя имя входа пользователя, затем значок " @ " и имя домена. По умолчанию доменное имя корневого домена выделено в выпадающем окне меню, независимо от того, в каком домене учетная запись была создана (выпадающий список будет также содержать имя домена, в котором вы создали эту учетную запись).

Также можно создавать дополнительные доменные суффиксы (та часть имени, которая стоит после знака @ ), которые будут появляться в выпадающем списке и могут быть использованы при образовании UPN, если вы их выберете (это делается при помощи консоли " *Active Directory – домены и доверие* " (" *Active Directory Domain and Trusts* ").

Существует только одно обязательное условие при этом — все UPN в лесу должны быть уникальными (т.е. не повторяться). Если учетная запись входа пользователя использует UPN для входа в систему Windows 2003, вам необходимо только указать UPN и пароль — более нет нужды помнить и указывать доменное имя. Другое преимущество данной системы именования состоит в том, что UPN часто соответствует электронному адресу пользователя, что опять уменьшает количество информации о пользователе, которую необходимо запоминать.

##### Локальные учетные записи

Каждый компьютер с операционными системами Windows NT/2000/XP/2003 (если это не сервер, являющийся контроллером домена) имеет локальную базу данных учетных записей, называемую базой данных SAM. Эти БД обсуждались при описании модели безопасности "Рабочая группа". Локальные пользователи и особенно группы используются при назначении прав доступа к ресурсам конкретного компьютера даже в доменной модели безопасности. Общие правила использования локальных и доменных групп для управления доступом будут описаны ниже.

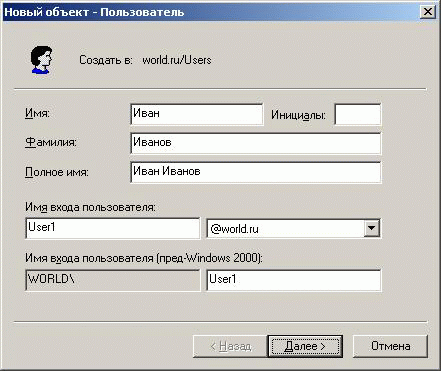
##### Управление доменными учетными записями пользователей

Доменные учетные записи пользователей (а также компьютеров и групп) хранятся в специальных контейнерах AD. Это могут быть либо стандартные контейнеры*Users* для пользователей и *Computers* для компьютеров, либо созданное администратором Организационное подразделение (ОП). Исключение составляют учетные записи контроллеров домена, они всегда хранятся в ОП с названием *Domain Controllers*.

Рассмотрим на примерах процесс создания учетных записей пользователей в БД Active Directory и разберем основные свойства доменных учетных записей. Учетные записи для компьютеров создаются в процессе включения компьютера в домен.

##### Создание доменной учетной записи

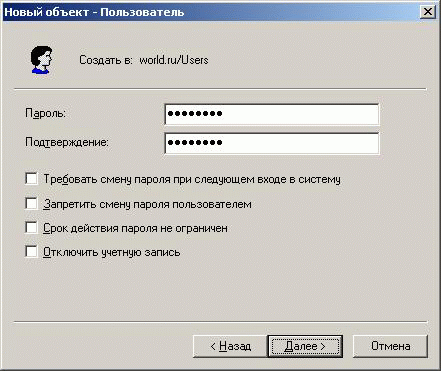
1. Откроем административную консоль " *Active Directory – пользователи и компьютеры* ".
2. Щелкнем правой кнопкой мыши на контейнере, в котором будем создавать учетную запись, выберем в меню команду " *Создать* " и далее — " *Пользователь* ".
3. Заполним поля " *Имя* ", " *Фамилия* ", например, " *Иван* " и " *Иванов* " (в английской версии — *First Name*, *Last Name* ), поле " *Полное имя* " ( *Full Name* ) заполнится само.
4. Введем " *Имя входа пользователя* " ( *User logon name* ), например, *User1*. К этому имени автоматически приписывается часть вида " @<имя домена> ", в нашем примере — " @world.ru " (полученное имя должно быть уникальным в масштабах леса).
5. В процессе формирования имени входа автоматически заполняется " *Имя входа пользователя (пред-Windows 2000)* " ( *User logon name (pre- Windows 2000)* ), создаваемое для совместимости с прежними версиями Windows (данное имя должно быть уникально в масштабе домена). В каждой организации должны быть разработаны схемы именования пользователей (по имени, фамилии, инициалам, должности, подразделению и т.д.) В нашем примере получится имя "*WORLD\User1* ". Нажмем кнопку " *Далее* " (рис. 6.43):



**Рис. 6.43.**

1. Вводим пароль пользователя (два раза, для подтверждения).
2. Укажем начальные требования к паролю:
   * Требовать смену пароля при следующем входе в систему (полезно в случае, когда администратор назначает пользователю начальный пароль, а затем пользователь сам выбирает пароль, известный только ему);
   * Запретить смену пароля пользователем (полезно и даже необходимо для учетных записей различных системных служб);
   * Срок действия пароля не ограничен (тоже используется для паролей учетных записей служб, чтобы политики домена не повлияли на функционирование этих служб, данный параметр имеет более высокий приоритет по сравнению с политиками безопасности);
   * Отключить учетную запись.

Нажмем кнопку " *Далее* " (рис. 6.44):



**Рис. 6.44.**

1. Получаем итоговую сводку для создаваемого объекта и нажимаем кнопку " *Готово* ".

**Внимание**! В упражнениях лабораторных работ дается задание настроить политики, которые сильно понижают уровень требований к паролям и полномочиям пользователей:

* отключается требование сложности паролей,
* устанавливается минимальная длина пароля, равная 0 (т.е. пароль может быть пустым),
* устанавливается минимальный срок действия паролей 0 дней (т.е. пользователь может в любой момент сменить пароль),
* устанавливается история хранения паролей, равная 0 (т.е. при смене пароля система не проверяет историю ранее используемых паролей),
* группе "Пользователи" дается право локального входа на контроллеры домена.

Данные политики устанавливаются исключительно для удобства выполнения упражнений, которые необходимо выполнять с правами простых пользователей на серверах-контроллерах домена. В реальной практике администрирования такие слабые параметры безопасности ни в коем случае устанавливать нельзя, требования к паролям и правам пользователей должны быть очень жесткими (политики безопасности обсуждаются далее в этом разделе).

Правила выбора символов для создания пароля:

* длина пароля — не менее 7 символов;
* пароль не должен совпадать с именем пользователя для входа в систему, а также с его обычным именем, фамилией, именами его родственников, друзей и т.д.;
* пароль не должен состоять из какого-либо слова (чтобы исключить возможность подбора пароля по словарю);
* пароль не должен совпадать с номером телефона пользователя (обычного или мобильного), номером его автомобиля, паспорта, водительского удостоверения или другого документа;
* пароль должен быть комбинацией букв в верхнем и нижнем регистрах, цифр и спецсимволов (типа @#$%^\*&()\_+ и т.д.).

И еще одно правило безопасности — регулярная смена пароля (частота смены зависит от требований безопасности в каждой конкретной компании или организации). В доменах Windows существует политика, определяющая срок действия паролей пользователей.

##### Обзор свойств учетных записей пользователей

Свойства учетной записи пользователя содержат большой набор различных параметров, размещенных на нескольких закладках при просмотре в консоли " *Active Directory – пользователи и компьютеры* ", причем при установке различных программных продуктов набор свойств может расширяться.

Рассмотрим наиболее важные с точки зрения администрирования свойства.

Откроем консоль " *Active Directory – пользователи и компьютеры* " и посмотрим свойства только что созданного нами пользователя.

Закладка " *Общие* ". На данной закладке содержатся в основном справочные данные, которые могут быть очень полезны при поиске пользователей в лесу AD. Наиболее интересные из них:

* " *Имя* "
* " *Фамилия* "
* " *Выводимое имя* "
* " *Описание* "
* " *Номер телефона* "
* " *Электронная почта* "

Закладка " *Адрес* " — справочная информация для поиска в AD.

Закладка " *Учетная запись* " — очень важный набор параметров (параметры " *Имя входа пользователя* " и " *Имя входа пользователя (пред-Windows 2000)* " обсуждались выше при создании пользователя):

* кнопка " *Время входа* " — дни и часы, когда пользователь может войти в домен;
* кнопка " *Вход на…* " — список компьютеров, с которых пользователь может входить в систему (регистрироваться в домене);
* Поле типа чек-бокс " *Заблокировать учетную запись* " — этот параметр недоступен, пока учетная запись не заблокируется после определенного политиками некоторого количества неудачных попыток входа в систему (попытки с неверным паролем), служит для защиты от взлома пароля чужой учетной записи методом перебора вариантов; если будет сделано определенное количество неудачных попыток, то учетная запись пользователя автоматически заблокируется, поле станет доступным и в нем будет установлена галочка, снять которую администратор может вручную, либо она снимется автоматически после интервала, заданного политиками паролей;
* " *Параметры учетной записи* " (первые три параметра обсуждались выше):
  + " *Требовать смену пароля при следующем входе в систему* "
  + " *Запретить смену пароля пользователем* "
  + " *Срок действия пароля не ограничен* "
  + " *Отключить учетную запись* " — принудительное отключение учетной записи (пользователь не сможет войти в домен);
  + " *Для интерактивного входа в сеть нужна смарт-карта* " — вход в домен будет осуществляться не при помощи пароля, а при помощи смарт-карты (для этого на компьютере пользователя должно быть устройство для считывания смарт-карт, смарт-карты должны содержать сертификаты, созданные Центром выдачи сертификатов);
* " *Срок действия учетной записи* " — устанавливает дату, с которой данная учетная запись не будет действовать при регистрации в домене (этот параметр целесообразно задавать для сотрудников, принятых на временную работу, людей, приехавших в компанию в командировку, студентов, проходящих практику в организации и т.д.)

Закладки " *Телефоны* ", " *Организация* " — справочная информация о пользователе для поиска в AD.

Закладка " *Профиль* "

*Профиль* ( *profile* ) — это настройки рабочей среды пользователя. Профиль содержит: настройки рабочего стола (цвет, разрешение экрана, фоновый рисунок), настройки просмотра папок компьютера, настройки обозревателя Интернета и других программ (например, размещение папок для программ семейства Microsoft Office). Профиль автоматически создается для каждого пользователя при первом входе на компьютер. Различают следующие виды профилей:

* *локальные* — хранятся в папке " *Documents and Settings* " на том разделе диска, где установлена операционная система;
* *перемещаемые* (сетевые, или *roaming* ) — хранятся на сервере в папке общего доступа, загружаются в сеанс пользователя на любом компьютере, с которого пользователь вошел (зарегистрировался) в домен, давая возможность пользователю иметь одинаковую рабочую среду на любом компьютере (путь к папке с профилем указывается на данной закладке в виде адреса \\server\share\%username%, где server — имя сервера, share — имя папки общего доступа,%username% — имя папки с профилем; использование переменной среды системы Windows с названием %username% позволяет задавать имя папки с профилем, совпадающее с именем пользователя);
* *обязательные* ( *mandatory* ) — настройки данного типа профиля пользователь может изменить только в текущем сеансе работы в Windows, при выходе из системы изменения не сохраняются.

Параметр "Сценарий входа" определяет исполняемый файл, который при входе пользователя в систему загружается на компьютер и исполняется. Исполняемым файлом может быть пакетный файл ( .bat, .cmd ), исполняемая программа (.exe, .com), файл сценария (.vbs, js).

Закладка " *Член групп* " — позволяет управлять списком групп, в которые входит данный пользователь.

Закладка " *Входящие звонки* ".

Управление доступом пользователя в корпоративную систему через средства удаленного доступа системы Windows Server (например, через модем или VPN-соединение). В *смешанном режиме* домена Windows доступны только варианты " *Разрешить доступ* " и " *Запретить доступ* ", а также параметры обратного дозвона ("*Ответный вызов сервера* "). В режимах " *Windows 2000 основной* " и " *Windows 2003* " доступом можно управлять с помощью политик сервера удаленного доступа (не надо путать с групповыми политиками). Подробнее данный вопрос обсуждается в разделе, посвященном средствам удаленного доступа.

Закладки " *Профиль служб терминалов* ", " *Среда* ", " *Сеансы* ", " *Удаленное управление* " — данные закладки управляют параметрами работы пользователя на сервере терминалов:

* управление разрешением пользователя работать на сервере терминалов;
* размещение профиля при работе в терминальной сессии,
* настройка среды пользователя в терминальной сессии (запуск определенной программы или режим рабочего стола, подключение локальных дисков и принтеров пользователя в терминальную сессию);
* управление сеансом пользователя на сервере терминалов (длительность сессии, тайм-аут бездействия сессии, параметры повторного подключения к отключенной сессии);
* разрешение администратору подключаться к терминальной сессии пользователя.

##### правление группами

Учетные записи групп, как и учетные записи пользователей, могут быть созданы либо в локальной базе SAM компьютера (сервера или рабочей станции), либо в доменной базе данных Active Directory.

Локальные группы простого сервера-члена домена или рабочей станции могут включать в себя и локальные учетные записи данного компьютера, и глобальные учетные записи любого пользователя или компьютера всего леса, а также доменные локальные группы "своего" домена и глобальные и универсальные группы всего леса.

Рассмотрим подробнее, какие группы могут создаваться в Active Directory.

В Active Directory группы различаются по типу (группы безопасности и группы распространения) и по области действия (локальные в домене, глобальные и универсальные).

Типы групп

* Группы безопасности — каждая группа данного типа, так же как и каждая учетная запись пользователя, имеет*идентификатор безопасности* ( *Security Identifier*, или *SID* ), поэтому группы безопасности используются для назначения разрешений при определении прав доступа к различным сетевым ресурсам.
* Группы распространения — группы этого типа не имеют идентификатора безопасности, поэтому не могут использоваться для назначения прав доступа, их главное назначение — организация списков рассылки для почтовых программ (например, для Microsoft Exchange Server).

Область действия групп

* **Локальные в домене** могут содержать — глобальные группы из любого домена, универсальные группы, глобальные учетные записи пользователей из любого домена леса, используются — при назначении прав доступа только к ресурсам "своего" домена;
* **Глобальные** могут содержать — только глобальные учетные записи пользователей "своего" домена, используются — при назначении прав доступа к ресурсам любого домена в лесу;
* **Универсальные** могут содержать — другие универсальные группы всего леса, глобальные группы всего леса, глобальные учетные записи пользователей из любого домена леса, используются — при назначении прав доступа к ресурсам любого домена в лесу.

В смешанном режиме домена универсальные группы недоступны для использования. В основном режиме или режиме Windows 2003 можно создавать и использовать универсальные группы. Кроме того, в основном режиме и режиме Windows 2003 глобальные группы могут включаться в другие глобальные группы, а доменные локальные группы могут включаться в другие доменные локальные.

Специфика универсальных групп заключается в том, что эти группы хранятся в Глобальном каталоге. Поэтому, если пользователь является членом универсальной группы, то при регистрации в домене ему обязательно должен быть доступен контроллер домена, являющийся *сервером глобального каталога*, в противном случае пользователь не сможет войти в сеть. Репликация между простыми контроллерами домена и *серверами глобального каталога* происходит достаточно медленно, поэтому любое изменение в составе универсальной группы требует больше времени для репликации, чем при изменении состава групп с другими областями действия.

Маркер доступа.

При регистрации в домене пользователю передается в его сессию на компьютере т.н. *маркер доступа* ( *Access Token* ), называемый иногда маркером безопасности. Маркер доступа состоит из набора идентификаторов безопасности — идентификатора безопасности (SID) самого пользователя и идентификаторов безопасности тех групп, членом которых он является. Впоследствии этот маркер доступа используется при проверке разрешений пользователя на доступ к различным ресурсам домена.

Стратегия создания и использования групп.

При создании и использовании групп следует придерживаться следующих правил:

1. Включать глобальные учетные записи пользователей ( **A** ccounts) в глобальные группы ( **G** lobal groups). Глобальные группы формируются обычно *по функциональным обязанностям сотрудников*.
2. Включать глобальные группы в доменные локальные или локальные на простом сервере или рабочей станции ( **L** ocal groups). Локальные группы формируются*на основе разрешений для доступа к конкретным ресурсам*.
3. Давать разрешения ( **P** ermissions) на доступ к ресурсам локальным группам.

По первым буквам английских слов эту стратегию часто обозначают сокращенно **AGLP**. В основном режиме и режиме Windows 2003 с использованием универсальных ( **U** niversal) групп эта стратегия может быть в более общем виде представлена как аббревиатура **AGG…GULL…LP**. Такой подход облегчает управление доступом к ресурсам по сравнению с назначением разрешений напрямую учетным записям пользователей. Например, при переходе сотрудника с одной должности на другую или из одного подразделения в другое достаточно соответствующим образом поменять его членство в различных группах, и разрешения на доступ к сетевым ресурсам автоматически будут назначены уже исходя из его новой должности.

Встроенные и динамически формируемые группы.

Кроме тех групп, которые создает администратор, на компьютерах локально или во всем домене существуют *встроенные группы*, созданные во время установки системы или создания домена. Кроме встроенных групп в процессе работы системы формируются *динамические группы*, состав которых меняется в зависимости от ситуации.

Перечислим наиболее часто используемые на практике встроенные и динамические группы.

|  |  |
| --- | --- |
| **Встроенные локальные группы (на рабочей станции или простом сервере).** | |
| **Название группы** | **Описание** |
| *Администраторы* | Могут выполнять все административные задачи на данном компьютере. Встроенная учетная запись *Администратор*, которая создается при установке системы, является членом этой группы. Если компьютер является членом домена, то в эту группу включается глобальная группа*Администраторы домена*. |
| *Операторы резервного копирования* | Члены группы могут выполнять вход на данный компьютер, выполнять резервное копирование и восстановление данных на этом компьютере, а также завершать работу этого компьютера. |
| *Администраторы DHCP*(создается при установке службы DHCP Server) | Члены этой группы могут администрировать службу DHCP Server. |
| *Операторы сетевой конфигурации* | Члены группы могут изменять настройки TCP/IP, а также обновлять и освобождать IP-адреса, назначаемые автоматически. |
| *Пользователи монитора производительности* | Члены группы могут следить за счетчиками производительности на конкретном сервере локально или удаленным образом. |
| *Пользователи журнала производительности* | Члены группы могут администрировать журналы производительности, счетчики и оповещения на конкретном сервере локально или удаленным образом. |
| *Опытные пользователи* | Члены группы могут создавать и модифицировать учетные записи пользователей, а также устанавливать программы на локальном компьютере, но не могут просматривать файлы других пользователей. Члены группы могут создавать и удалять локальные группы, а также добавлять и удалять пользователей в группах, которые они создали. Члены группы могут добавлять и удалять пользователей в группах*Опытные пользователи*, *Пользователи* и *Гости*. |
| *Операторы печати* | Члены группы могут управлять принтерами и очередями печати на конкретном сервере. |
| *Пользователи удаленного рабочего стола* | Членам группы разрешается выполнять подключение к удаленному рабочему столу компьютера. |
| *Пользователи* | Члены этой группы могут локально входить в систему на данном компьютере, работать с программами, сохранять документы и завершать работу данного компьютера. Они не могут устанавливать программы или вносить изменения в систему. Если компьютер является членом домена, то в эту группу включается глобальная группа *Пользователи домена*. В эту группу также включаются динамические группы*Интерактивные* и *Прошедшие проверку*. |
| **Встроенные доменные локальные группы.** | |
| **Название группы** | **Описание** |
| *Администраторы* | Членам группы предоставляются права администратора на всех контроллерах домена и в самом домене. Учетная запись *Администратор*, группы *Администраторы предприятия* и *Администраторы домена* являются членами данной группы. |
| *Операторы учетных записей* | Члены группы могут создавать, удалять и управлять учетными записями пользователей и группами. Они не могут модифицировать группу*Администраторы*, *Администраторы домена*, *Контроллеры домена* или любую из групп *Операторы*. |
| *Операторы резервного копирования* | Члены группы могут выполнять резервное копирование и восстановление данных на всех контроллерах домена, а также могут выполнять вход на контроллеры домена и завершать их работу. |
| *Администраторы DNS*(создается при установке службы DNS) | Члены группы имеют административный доступ к серверам DNS. |
| *Операторы сетевой конфигурации* | Члены группы могут изменять настройки TCP/IP на контроллерах доменов. |
| *Пользователи монитора производительности* | Члены группы могут следить за счетчиками производительности на контроллерах домена. |
| *Пользователи журнала производительности* | Члены группы могут управлять журналами производительности, счетчиками и оповещениями на контроллерах домена. |
| *Операторы печати* | Члены группы могут управлять работой принтеров домена |
| *Операторы сервера* | Члены группы могут выполнять большинство административных задач на контроллерах домена, за исключением изменения параметров безопасности. |
| *Пользователи* | Члены этой группы локально могут входить в систему на данном компьютере, работать с программами, сохранять документы и завершать работу данного компьютера. Они не могут устанавливать программы или вносить изменения в систему. Группа *Пользователи домена*является по умолчанию членом данной группы. |
| **Встроенные глобальные группы.** | |
| **Название группы** | **Описание** |
| *Администраторы домена* | Эта группа автоматически включается в локальную в домене группу *Администраторы*, поэтому члены группы *Администраторы домена* могут выполнять административные задачи на любом компьютере данного домена. Учетная запись *Администратор* включается в эту группу по умолчанию. |
| *Компьютеры домена* | Все контроллеры, серверы и рабочие станции домена являются членами этой группы. |
| *Контроллеры домена* | Все контроллеры домена являются членами этой группы. |
| *Пользователи домена* | Все глобальные учетные записи домена и входят в эту группу. Эта группа автоматически включается в локальную доменную группу*Пользователи*. |
| *Администраторы предприятия*(создается только в корневом домене леса) | Эта группа предназначена для пользователей, которые должны иметь права администратора в масштабах всего леса. *Администраторы предприятия* автоматически включается в группу *Администраторы* на всех контроллерах домена в данном лесу. |
| *Администраторы схемы* (создается только в корневом домене леса) | Члены этой группы могут изменять схему Active Directory. |
| **Динамические группы.** | |
| **Название группы** | **Описание** |
| *Интерактивные* | В эту группу включается учетная запись любого пользователя, который локально вошел в систему на данном компьютере. |
| *Прошедшие проверку* | Любой пользователь, зарегистрировавшийся в данном домене или домене, имеющим с данным доменом доверительные отношения. |
| *Все* | Любая учетная запись, включая те, которые не прошли проверку на контроллерах доменов. |

#### Управление Организационными подразделениями, делегирование полномочий

Назначение *Организационных подразделений* ( *ОП*, *Organizational Units*, *OU* ) — организация иерархической структуры объектов AD внутри домена. Как правило, иерархия ОП в домене отражает организационную структуру компании.

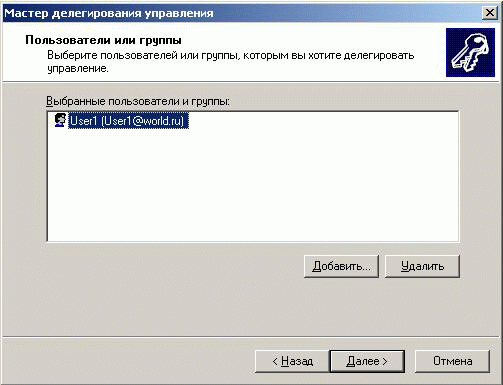
На практике использование ОП (кроме иерархической организации объектов) сводится к двум задачам:

* делегирование административных полномочий на управление объектами ОП какому-либо пользователю или группе пользователей;
* применение групповых политик к объектам, входящим в ОП.

Делегирование административных полномочий на управление объектами ОП какому-либо пользователю или группе позволяет в больших организациях распределить нагрузку по администрированию учетными записями между различными сотрудниками, не увеличивая при этом количество пользователей, имеющих административные права на уровне всего домена.

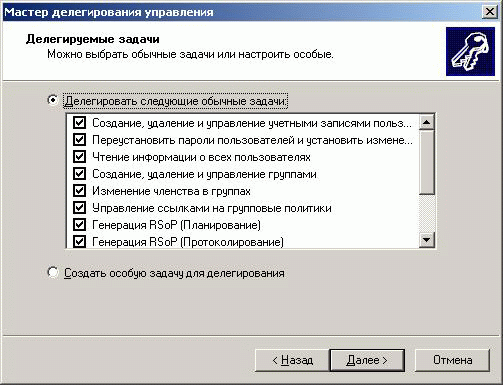
Рассмотрим на примере процедуру предоставления какому-либо пользователю административных прав на управление ОП.

1. Откроем консоль " *Active Directory – пользователи и компьютеры* ".
2. Создадим в домене подразделение, скажем, с именем OU-1, переместим в это ОП несколько имеющихся в домене учетных записей (или создадим новые).
3. Щелкнем правой кнопкой мыши на подразделении OU-1 и выберем пункт меню " *Делегирование управления…* ". Запустится " *Мастер делегирования управления*"
4. Выберем пользователя (или группу), которому будем делегировать управление данным ОП. Пусть это будет пользователь User1 (рис. 6.45). Нажмем " *Далее* ".



**Рис. 6.45.**

1. Выберем набор административных задач, которые делегируются данному пользователю (рис. 6.46):



**Рис. 6.46.**

1. По завершении мастера — нажмем кнопку " *Готово* ".

Если теперь войти в систему на контроллере домена с учетной записью User1 (при условии, что у пользователя User1 есть права локального входа в систему на контроллере домена), запустить консоль " *Active Directory – пользователи и компьютеры* ", то пользователь User1 сможет выполнять любые операции с объектами организационного подразделения OU-1.

Кроме удобных консолей с графическим интерфейсом система Windows 2003 оснащена мощным набором утилит командной строки для управления объектами Active Directory:

* dsadd — добавляет объекты в каталог;
* dsget — отображает свойства объектов в каталоге;
* dsmod — изменяет указанные атрибуты существующего объекта в каталоге;
* dsquery — находит объекты в каталоге, удовлетворяющие указанным критериям поиска;
* dsmove — перемещает объект из текущего местоположения в новое родительское место;
* dsrm — удаляет объект или все поддерево ниже объекта в каталоге.

Примеры.

1. Создание подразделения OU-New в домене world.ru:

dsadd ou "ou=OU-New,dc=world,dc=ru"

1. Создание пользователя User-New в подразделении OU-New в домене world.ru:

dsadd user "cn=User-New,ou=OU-New,dc=world,dc=ru"

1. Модификация параметра " *Номер телефона* " у пользователя User-New:

dsmod user "cn=User-New,ou=OU-New,dc=world,dc=ru" –tel 123-45-67

1. Получение списка пользователей домена, у которых имя начинается с символа "u":

dsquery user -name u\*

Далее рассмотрим применение групповых политик (как для отдельных ОП, так и для других структур Active Directory).

**Групповые политики: назначение, состав, стандартные политики домена, порядок применения политик (локальные, сайт, домен, ОП), применение политик и права доступа, наследование и блокировка применения**

Управление рабочими станциями, серверами, пользователями в большой организации — очень трудоемкая задача. Механизм*Групповых политик* ( *Group Policy* ) позволяет автоматизировать данный процесс управления. С помощью групповых политик (*ГП* ) можно настраивать различные параметры компьютеров и пользовательской рабочей среды сразу в масштабах сайта AD, домена, организационного подразделения (детализацию настроек можно проводить вплоть до отдельного компьютера или пользователя). Настраивать можно широкий набор параметров — сценарии входа в систему и *завершения сеанса работы* в системе, параметры *Рабочего стола* и *Панели управления*, размещения личных папок пользователя, настройки безопасности системы (политики паролей, управления учетными записями, аудита доступа к сетевым ресурсам, управления сертификатами и т.д.), развертывания приложений и управления их жизненным циклом.

Каждый *объект групповых политик* ( *GPO*, *Group Policy Object* ) состоит из двух частей: *контейнера групповых политик* (GPC,*Group Policy Container* ) хранящегося в БД Active Directory, и *шаблона групповых политик* ( *GPT*, *Group Policy Template* ), хранящегося в файловой системе контроллера домена, в подпапках папки SYSVOL. Место, в котором хранятся шаблоны политик, — это папка %systemroot%\SYSVOL\sysvol\<имя домена>\Policies, и имя папки шаблона совпадает с глобальным уникальным идентификатором (GUID) *объекта Групповая политика*.

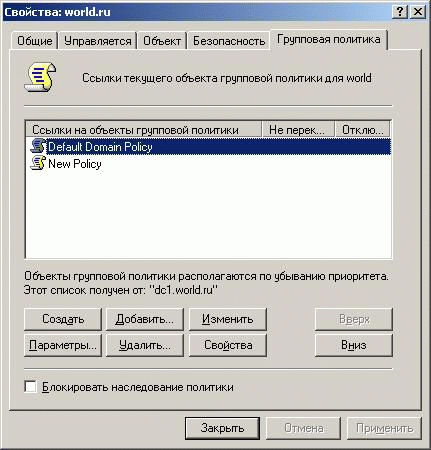
Каждый объект политик содержит два раздела: конфигурация компьютера и конфигурация пользователя. Параметры этих разделов применяются соответственно либо к настройкам компьютера, либо к настройкам среды пользователя.

Задание параметров групповых политик производится Редактором групповых политик, который можно открыть в консоли управления соответствующим объектом AD.

Каждый объект политик может быть привязан к тому или иному объекту AD — сайту, домену или организационному подразделению (а также к нескольким объектам одновременно).

Задание параметров групповых политик производится Редактором групповых политик, который можно открыть в консоли управления соответствующим объектом AD (" *Active Directory – сайты и службы* ", " *Active Directory – пользователи и компьютеры* ", локальная политика компьютера редактируется консолью gpedit.msc, запускаемой из командной строки). На рис. 6.47 показана закладка " *Групповые политики* " свойств домена world.ru. На данной закладке можно выполнить следующие действия:

* кнопка " *Создать* " — создать новый объект ГП;
* кнопка " *Добавить* " — привязать к данному объекту AD существующий объект ГП;
* кнопка " *Изменить* " — открыть редактор групповых политик для выбранного объекта ГП;
* кнопка " *Параметры* " — запретить перекрывание (поле " *Не перекрывать* ") параметров данной объекта ГП другими политиками или блокировку на более низком уровне иерархии AD или отключить (поле " *Отключить* ") данный объект ГП;
* кнопка " *Удалить* " — удалить совсем выбранный объект ГП или удалить привязку объекта ГП к данному уровню AD;
* кнопка " *Свойства* " — отключить компьютерный или пользовательский разделы политики или настроить разрешения на использование данного объекта ГП;
* поле " *Блокировать наследование политики* " — запретить применение политик, привязанных к более высоким уровням иерархии AD;
* кнопки " *Вверх* " и " *Вниз* " — управление порядком применения политик на данном уровне AD (политики, расположенные в списке выше, имеют более высокий приоритет).



**Рис. 6.47.**

При загрузке компьютера и аутентификации в домене к нему применяются компьютерные разделы всех привязанных политик. При входе пользователя в систему к пользователю применяется пользовательский раздел всех групповых политик. Политики, привязанные к некоторому уровню иерархии объектов AD (сайта, домена, подразделения) наследуются всеми объектами AD, находящимися на более низких уровнях. Порядок применения политик:

* локальная политика;
* политики сайта Active Directory;
* политики домена;
* политики организационных подразделений.

Если в процессе применения политик какие-либо параметры определяются в различных политиках, то действующими значениями параметров будут значения, определенные позднее.

Имеются следующие методы управления применением групповых политик (см. рис. 6.47):

* блокировка наследования политик на каком либо уровне иерархии AD;
* запрет блокировки конкретного объекта групповых политик;
* управление приоритетом применения политик на конкретном уровне AD (кнопками " *Вверх* " и " *Вниз* ");
* разрешение на применение политик (чтобы политики какого-либо объекта ГП применялись к пользователю или компьютеру, данный пользователь или компьютер должен иметь разрешения на этот объект ГП " *Чтение* " и " *Применение групповой политики* ").

Кроме применения политик в момент загрузки компьютера или входа пользователя в систему, каждый компьютер постоянно запрашивает обновленные политики на контроллерах домена, загружает их и применяет обновленные параметры (и к пользователю, и к компьютеру). Рабочие станции домена и простые серверы запрашивают обновления каждые 90 ± 30 минут, контроллеры домена обновляют свои политики каждые 5 минут. Обновить набор политик на компьютере можно принудительно из командной строки командой gpupdate (на компьютерах с системами Windows XP/2003) или командами " secedit /refreshpolicy machine\_policy" и " secedit /refreshpolicy user\_policy " (на компьютерах с системой Windows 2000).

На практических занятиях необходимо изучить работу редактора групповых политик, ознакомиться с набором параметров стандартных политик домена и выполнить задания по настройке рабочей среды пользователей с помощью групповых политик.

**Управление приложениями**

Рассмотрим немного подробнее использование групповых политик для развертывания приложений в сетях под управлением Active Directory.

Групповые политики могут использоваться для установки прикладных программ в масштабах всего домена или отдельного организационного подразделения.

Используются следующие способы управления установкой приложений:

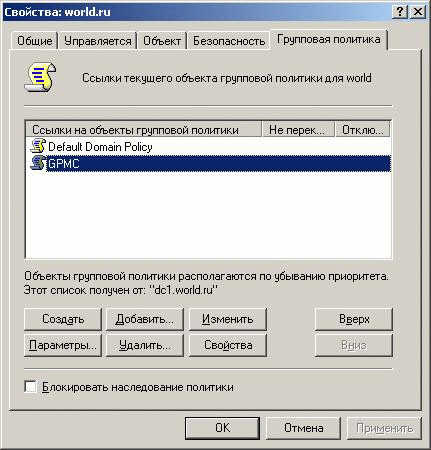
* **назначение приложений компьютерам** (при данном способе приложение, назначенное компьютеру, автоматически устанавливается при загрузке компьютера);
* **назначение приложений пользователям** (приложение устанавливается при первом вызове данного приложения — при открытия ярлычка приложения или файла, соответствующего данному приложению);
* **публикация приложений пользователям** (название приложения добавляется к списку доступных для установки программ в окне " *Установка и удаление программ* " в *Панели управления* ).

С помощью политик можно управлять установкой приложений, которые устанавливаются с помощью компоненты *Windows Installer*, т.е. для них установочный пакет должен быть создан в формате файла с расширением " .msi ". Если приложение можно установить только с помощью установочной программы типа setup.exe илиinstall.exe, то такие приложения *могут быть опубликованы* (но не назначены) после создания файла типа " .*zap* ", в котором заданны соответствующие параметры, необходимые для публикации средствами ГП.

Рассмотрим на примерах процессы назначения и публикации приложений.

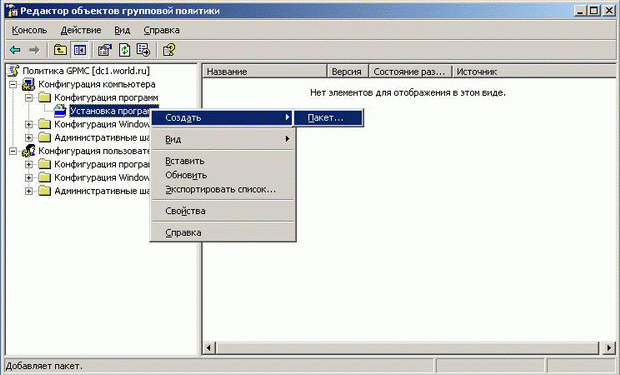
Пример 1. Назначение пакета *Group Policy Management Console* (" *Консоль управления групповыми политиками* ") всем компьютерам домена world.ru.

1. Откроем закладку " *Групповые политики* " свойств домена. Создадим новый объект ГП с именем " *GPMC* " (рис. 6.48).



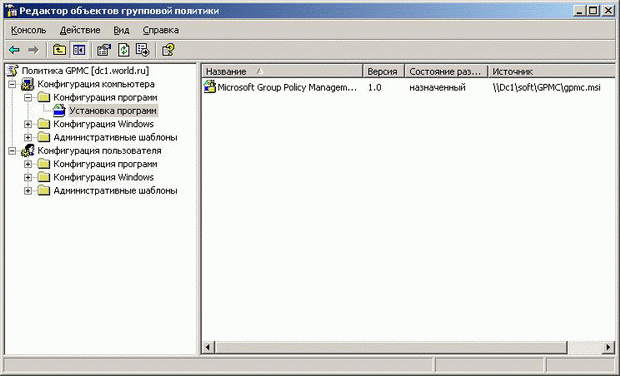
**Рис. 6.48.**

1. Откроем редактор политик для политики *GPMC*, откроем " *Конфигурация компьютера* ", " *Конфигурация программ* ", на параметре " *Установка программ* " щелкнем правой кнопкой мыши и выберем " *Создать — Пакет* " (рис. 6.49):



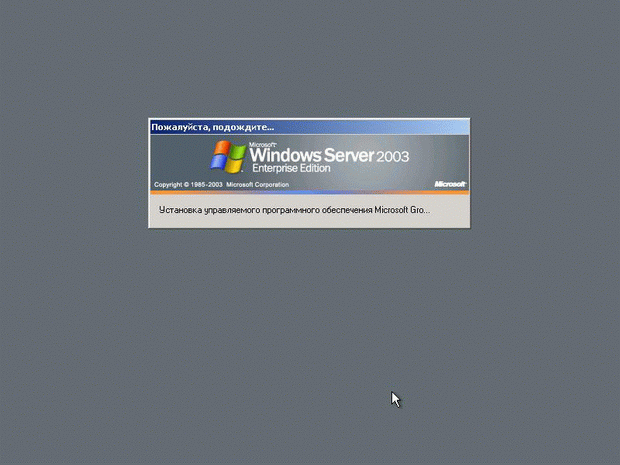
**Рис. 6.49.**

1. Укажем сетевой путь к пакету " \\DC1\Soft\GPMC\gpmc.msi ". Выберем метод развертывания " *Назначенный* ", нажмем " *ОК* ". В окне редактора политик появится значение параметра (рис. 6.50):



**Рис. 6.50.**

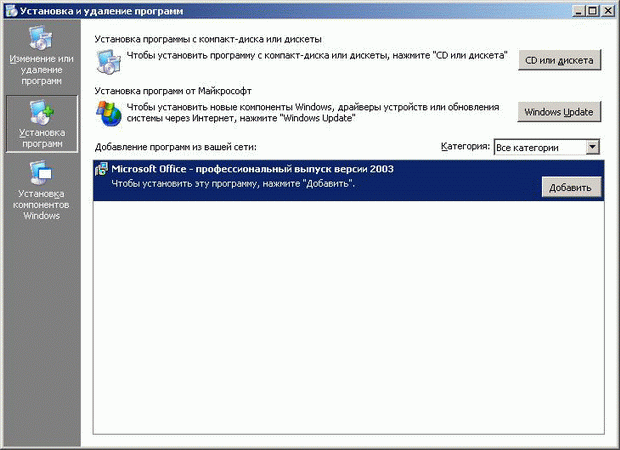
1. При загрузке компьютера в домене в процессе применения политик будет установлен данный программный пакет (рис. 6.51):



**Рис. 6.51.**

Пример 2. Публикация пакета *Microsoft Office 2003* всем пользователям домена world.ru.

1. Откроем закладку " *Групповые политики* " свойств домена. Создадим новый объект ГП с именем " *MS Office 2003* ".
2. Откроем редактор политик для политики *MS Office 2003*, откроем " *Конфигурация пользователя* ", " *Конфигурация программ* ", на параметре " *Установка программ* " щелкнем правой кнопкой мыши и выберем " *Создать — Пакет* ".
3. Укажем сетевой путь к пакету " \\DC1\Soft\Office 2003\PRO11.msi ". Выберем метод развертывания " *Публичный* ", нажмем " *ОК* ".
4. После применения политик откроем *Панель управления*, выберем " *Установка и удаление программ* ", нажмем кнопку " *Установка программ* ", в окне доступных для установки программ появится название пакета " *Microsoft Office 2003* " (рис. 6.52).



**Рис. 6.52.**

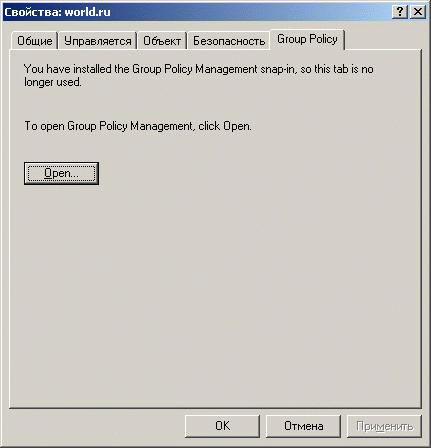
**Group Policy Management Console**

В качестве примера установки пакета с помощью назначения мы выбрали пакет *MS Group Policy Management Console* (*Консоль управления групповыми политиками* ). Установочный комплект можно найти в Центре загрузки сайта корпорации Microsoft (пакет распространяется бесплатно).

Рассмотрим теперь подробнее, как работает этот пакет.

Во-первых, установить его можно на компьютер с системам Windows XP/2003. При этом управлять политиками пакет может и в доменах под управлением Windows 2000.

Во-вторых, при просмотре свойств какого либо домена или ОП закладка "Групповые политики" после установки GPMC выглядит по-другому (рис. 6.53):

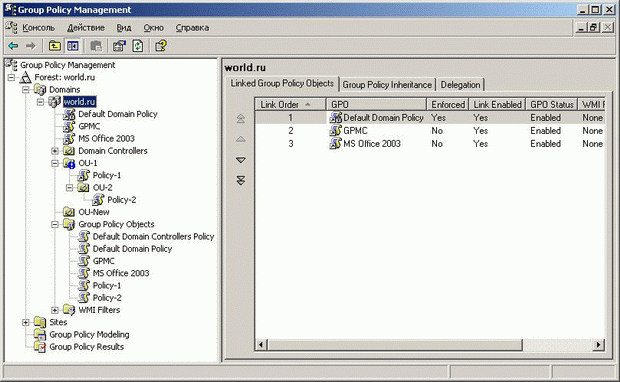


**Рис. 6.53.**

На этой закладке вместо списка политик и множества кнопок теперь всего одна кнопка " *Open* " (" *Открыть* ").

Отметим основные преимущества этой консоли по сравнению с базовыми возможностями системы.

1. Наглядное отображение иерархии внутри домена со всеми объектами ГП, привязанными к разным уровням иерархии ОП (рис. 6.54):



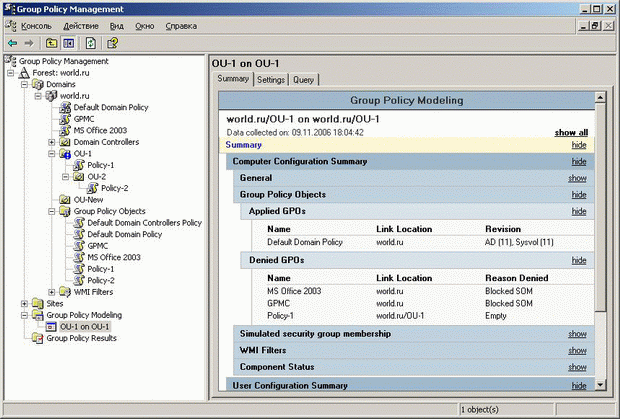
**Рис. 6.54.**

На рисунке хорошо видна вся иерархия подразделений внутри домена world.ru. Причем на каждом уровне отображается список политик, привязанных к данному уровню. Например, на уровне домена привязаны политики: стандартная политика домена, политика *GPMC* (назначение пакета GPMC) и политика *MS Office 2003*(публикация пакета MS Office). На уровне подразделения OU-1 включено *блокирование наследования* политик (синий значок с восклицательным знаком). Стандартная политика домена Default Domain Policy имеет свойство " *Не перекрывать* " (небольшой значок справа от стрелки на пиктограмме объекта ГП). Включение параметра " *Не перекрывать* " в этой консоли делается так: щелкнуть правой кнопкой мыши на объекте ГП и в контекстном меню выбрать пункт "*Enforce* ".

В контейнере " *Group Policy Objects* " приведен полный список всех объектов ГП.

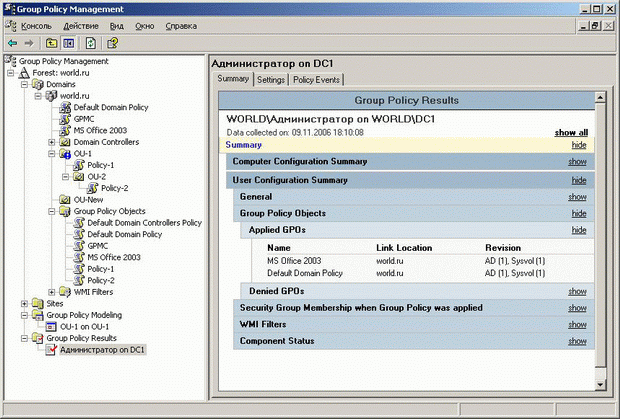
Для вызова редактора политик нужно щелкнуть правой кнопкой мыши на объекте ГП и в контекстном меню выбрать пункт " *Edit* ".

В разделе " *Group Policy Modeling* " можно определить, какой набор политики будет применяться на том или ином уровне иерархии AD (на рис. 6.55 выведен список политик, примененных к подразделению OU-1):



**Рис. 6.55.**

В разделе " *Group Policy Results* " можно определить набор параметров, примененных к определенному пользователю или компьютеру в результате наложения всех политик (рис. 6.56, список политик для пользователя *Администратор* ):



**Рис. 6.56.**

**6.4 Система безопасности (протокол Kerberos, настройка параметров системы безопасности)**

**Протокол Kerberos**

Протокол *Kerberos* был создан более десяти лет назад в Массачусетском технологическом институте в рамках проекта *Athena*. Однако общедоступным этот протокол стал, начиная с версии 4. После того, как специалисты изучили новый протокол, авторы разработали и предложили очередную версию — Kerberos 5, которая была принята в качестве стандарта IETF. Требования реализации протокола изложены в документе RFC 1510, кроме того, в спецификации RFC 1964 описывается механизм и формат передачи жетонов безопасности в сообщениях Kerberos.

Протокол Kerberos предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищённой среде, а передаваемые пакеты могут быть перехвачены и модифицированы. Другими словами, протокол идеально подходит для применения в Интернет и аналогичных сетях.

Основная концепция протокола Kerberos очень проста — если есть секрет, известный только двоим, то любой из его хранителей может с лёгкостью удостовериться, что имеет дело со своим напарником. Для этого ему достаточно проверить, знает ли его собеседник общий секрет.

Протокол Kerberos решает эту проблему средствами криптографии с секретным ключом. Вместо того, чтобы сообщать друг другу пароль, участники сеанса связи обмениваются криптографическим ключом, знание которого подтверждает личность собеседника. Но чтобы такая технология оказалась работоспособной, необходимо, чтобы общий ключ был симметричным, т.е., он должен обеспечивать как шифрование, так и дешифрование информации. Тогда один из участников использует его для шифрования данных, а другой с помощью этого ключа извлекает их.

Простой протокол аутентификации с секретным ключом вступает в действие, когда кто-то стучится в сетевую дверь и просит впустить его. Чтобы доказать своё право на вход, пользователь предъявляет *аутентификатор* ( *authenticator* ) в виде набора данных, зашифрованного секретным ключом. Получив *аутентификатор*, "привратник" расшифровывает его и проверяет полученную информацию, чтобы убедиться в успешности дешифрования. Разумеется, содержание набора данных должно постоянно меняться, иначе злоумышленник может просто перехватить пакет и воспользоваться его содержимым для входа в систему. Если проверка прошла успешно, то это значит, что посетителю известен секретный код, а так как этот код знает только он и привратник, следовательно, пришелец на самом деле тот, за кого себя выдаёт.

При использовании простых протоколов, типа описанного выше, возникает одна важная проблема. Если каждому клиенту для поддержания связи с каждой службой требуется индивидуальный ключ, и такой же ключ нужен каждой службе для каждого клиента, то проблема обмена ключами быстро приобретает предельную остроту. Необходимость хранения и защиты такого множества ключей на огромном количестве компьютеров создаёт невероятный риск для всей системы безопасности.

Само название протокола Kerberos говорит о том, как здесь решена проблема управления ключами. *Цербер* (или *Кербер* ) — персонаж греческой мифологии. Этот свирепый пёс о трёх головах, по поверьям греков, охраняет врата подземного царства мёртвых. Трём головам Цербера в протоколе Kerberos соответствуют три участника безопасной связи:

* **Клиент** — система (пользователь), делающий запрос;
* **Сервер** — система, которая обеспечивает сервис для систем, чью подлинность нужно подтвердить.
* **Центр распределения ключей** ( *Key Distribution Center*, *KDC* ) — сторонний посредник между клиентом и сервером, который ручается за подлинность клиента. В среде Windows , начиная с Windows 2000, в роли *KDC* выступает контроллер домена со службой каталогов Active Directory.

В среде Kerberos для входа в систему пользователь должен предоставить свое имя пользователя, пароль и имя домена (часто упоминаемое как *Realm*, или " *Сфера*", в словаре Kerberos), в который он хочет войти. Эта информация посылается *KDC*, который устанавливает подлинность пользователя. Если пользователь подлинный, ему предоставляется нечто, называемое " *билет на получение билета* " ( *ticket-granting ticket*, *TGT* ).

Однако, если вам необходим доступ к конкретному серверу, вам также необходим билет для этого сервера или вы не сможете создать сеанс связи с ним.

Когда вы хотите получить доступ к серверу, вы сначала должны обратиться к *KDC*, предъявить свой билет TGT, как подтверждение своей подлинности, а затем уже запросить " *билет сеанса* " для сервера, с которым вам необходим контакт. Если вы аутентифицированы, вы сможете получить доступ к серверу в соответствии с правами, которыми обладаете. Билет сеанса и TGT, которые вы получаете, имеют ограниченное время действия, которое может настраиваться в групповой политике. Значения по умолчанию составляют для TGT (также упоминаемого как билет пользователя) — 7 дней, а для билета сеанса (также упоминаемого как билет службы) — 10 часов.

В среде с одним доменом аутентификация Kerberos осуществляется очень просто. Однако в среде со многими доменами, этот процесс происходит в несколько этапов. Причина в том, что когда вы пытаетесь получить билет сессии для сервера, он должен быть получен от *KDC* того домена, в котором расположен сервер. Поэтому вы должны будете получить несколько билетов сессии, для прохождения цепочки доверительных отношений по пути к *KDC*, к которому вам нужно получить доступ.

Пример, приведенный ниже, демонстрирует шаги, необходимые для того, чтобы клиент, расположенный в домене it.company.ru, получил доступ к серверу в доменеsales.company.ru:

* клиент входит в систему как пользователь в домене it.company.ru и получает соответствующий TGT;
* клиент хочет взаимодействовать с сервером в домене sales.company.ru, он контактирует с *KDC* в домене it.company.ru и запрашивает билет сеанса для *KDC* в домене company.ru;
* после получения этого билета он контактирует с *KDC* в домене company.ru и запрашивает билет сеанса для *KDC* в домене sales.company.ru;
* после получения этого билета он контактирует с *KDC* в домене sales.company.ru и запрашивает билет для сервера, к которому ему необходим доступ;
* получив билет сессии для доступа к серверу, клиент имеет доступ к нему в соответствии с имеющимися у него разрешениями.

**Настройка параметров безопасности (Шаблоны безопасности, Анализ и настройка безопасности)**

Управлению безопасностью в сетях Microsoft Windows посвящено немало учебных курсов и хороших книг. В предыдущих разделах мы уже касались политик безопасности, относящихся к учетным записям пользователей (параметры длины и сложности пароля, параметры блокировки учетных записей) и параметрам прав пользователей (в частности, локальный вход в систему на сервере для выполнения лабораторных работ в компьютерном классе).

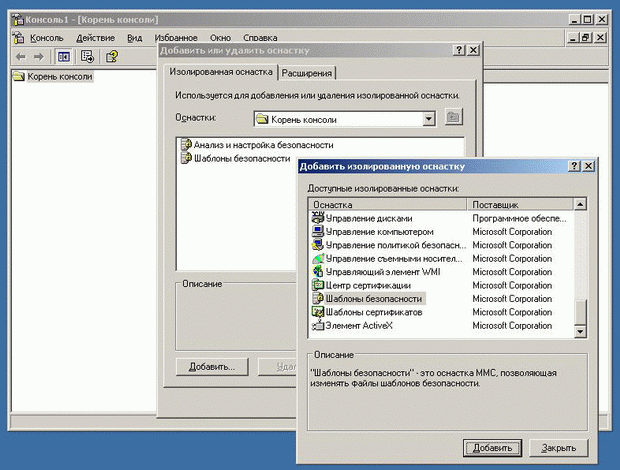
Оставим подробное изучение безопасности сетей Microsoft за рамками данного курса, но при этом рассмотрим работу с очень полезными оснастками, которые могут помочь начинающему сетевому администратору ознакомиться с некоторыми стандартными шаблонами политик безопасности, которые имеются в самой системе Windows Server, и проводить анализ и текущих настроек сервера в сравнении со этими стандартными шаблонами.

1. Сначала откроем чистую консоль mmc.

Кнопка " *Пуск* " — " *Выполнить* " — mmc — кнопка " *ОК* ".

1. Добавим в новую консоль оснастки " *Шаблоны безопасности* " и " *Анализ и настройка безопасности* ".

Меню " *Консоль* " — " *Добавить или удалить оснастку* " — кнопка " *Добавить* " — выбрать оснастку " *Анализ и настройка безопасности* " — кнопка " *Добавить* " — выбрать оснастку " *Шаблоны безопасности* " — кнопка " *Добавить* " — кнопка "*Закрыть* " — кнопка " *ОК* " (рис. 6.57).



**Рис. 6.57.**

В полученной консоли (ее можно будет сохранить и использовать в дальнейшем неоднократно) можно делать следующее:

* изучить параметры стандартных шаблонов безопасности (оснастка "Шаблоны безопасности") и даже попробовать сконструировать собственные шаблоны на основе стандартных (можно сохранить какой-либо шаблон с другим именем и изменить какие-либо параметры шаблона);
* провести анализ (сравнение) текущих параметров безопасности сервера (оснастка " *Анализ и настройка безопасности* ").

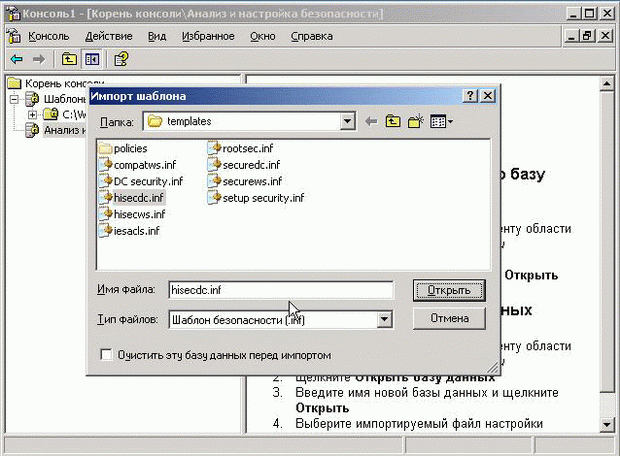
Приведем краткие характеристики стандартных шаблонов безопасности:

* **DC security** — используемые по умолчанию параметры безопасности контроллера домена;
* **securedc** — защищенный контроллер домена (более высокие требования к безопасности по сравнению с шаблоном *DC security*, отключается использование метода аутентификации *LanManager* );
* **hisecdc** — контроллер домена с высоким уровнем защиты (более высокие требования к безопасности по сравнению с шаблоном *securedc*, отключается метод аутентификации *NTLM*, включается требование цифровой подписи пакетов SMB);
* **compatws** — совместимая рабочая станция или совместимый сервер (ослабляет используемые по умолчанию разрешения доступа группы "Пользователи" к реестру и к системным файлам для того, чтобы приложения, не сертифицированные для использования в данной системе, могли работать в ней);
* **securews** — защищенная рабочая станция или защищенный сервер (аналогичен шаблону *securedc*, но предназначен для применения к рабочим станциям и простым серверам);
* **hisecws** — рабочая станция или защищенный сервер с высоким уровнем защиты (аналогичен шаблону *hisecdc*, но предназначен для применения к рабочим станциям и простым серверам);
* **setup security** — первоначальные настройки по умолчанию (параметры, устанавливаемые во время инсталляции системы);
* **rootsec** — установка стандартных (назначаемых во время инсталляции системы) NTFS-разрешений для папки, в которую установлена операционная система;

Теперь на примере рассмотрим, как проводить анализ настроек безопасности.

1. Откроем базу данных, в которой будут сохраняться настройки проводимого нами анализа.

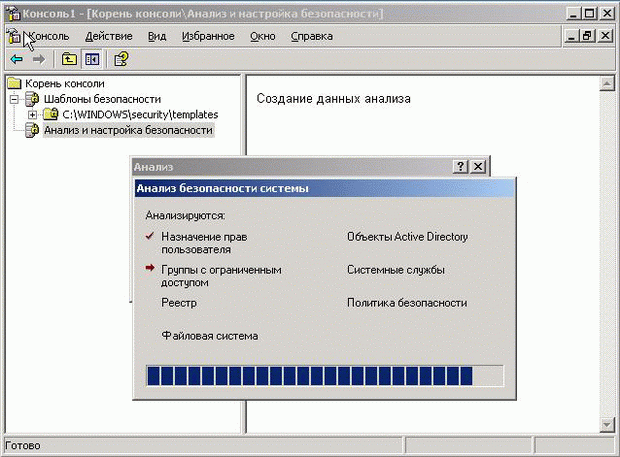
Щелкнем правой кнопкой мыши на значке оснастки " *Анализ и настройка безопасности* ", выберем " *Открыть базу данных* ", укажем путь и название БД (по умолчанию БД создается в папках профиля того администратора, который проводит анализ), нажмем кнопку " *Открыть* ", выберем нужный нам шаблон (например, *hisecdc* ) и нажмем " *ОК* " (рис. 6.58):



**Рис. 6.58.**

1. Выполним анализ настроек безопасности.

Щелкнем правой кнопкой мыши на значке оснастки " *Анализ и настройка безопасности* ", выберем " *Анализ компьютера* ", укажем путь и название файла с журналом ошибок (т.е. протоколом проведения анализа), нажмем "ОК", будет выполнено сравнение текущих настроек с параметрами шаблона (рис. 6.59):



**Рис. 6.59.**

1. Теперь можно провести уже настоящий анализ настроек безопасности.

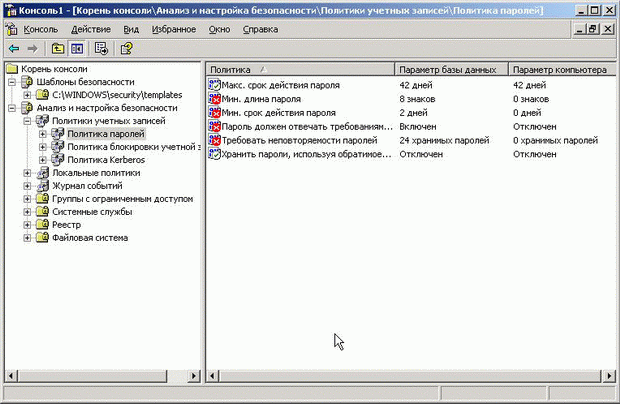
Откроем любой раздел оснастки (например, " *Политики паролей* ", рис. 6.60):

На рисунке сразу видны расхождения между настройками нашего сервера (столбец " *Параметр компьютера* ") и настройками шаблона (столбец " *Параметр базы данных* ") — видно, как мы понизили настройке безопасности для проведения практических занятий.

Аналогично проводится анализ всех остальных разделов политик безопасности.

Этой же оснасткой можно одним действием привести настройки нашего компьютера в соответствии с параметрами шаблона (щелкнуть правой кнопкой мыши на значке оснастки " *Анализ и настройка безопасности* ", выбрать " *Настроить компьютер* "). Не рекомендуем это делать, не изучив в деталях, какие последствия это может повлечь для всей сети. Высокие требования к параметрам безопасности препятствуют работе в домене Active Directory компьютеров с системами Windows 95/98/ME/NT. Например, данные системы поддерживают уровень аутентификации *NTLM* версии 2 (который назначается шаблонами *hisecdc* и *hisecws* ) только при проведении определенных настроек на компьютерах со старыми системами. Поэтому, прежде чем принимать решение об установке более высоких параметров безопасности в сети, необходимо тщательно изучить состав сети, какие требования к серверам и рабочим станциям предъявляют те или иные шаблоны безопасности, предварительно установить нужные обновления и настроить нужные параметры на "старых" системах и только после этого применять к серверам и рабочим станциям Windows 2000/XP/2003 шаблоны с высокими уровнями сетевой безопасности.

Заметим дополнительно, что данные оснастки имеются не только на серверах, но и на рабочих станциях под управлением Windows 2000/XP Professional, и они позволяют производить аналогичный анализ и настройки на рабочих местах пользователей.



**Рис. 6.60.**

**Резюме**

Первая часть данного раздела описывает задачи служб каталогов корпоративной сети и основные понятия служб каталогов Active Directory:

* домен;
* дерево;
* лес;
* организационное подразделение.

Вторая часть дает углубленные знания по логической и физической структуре службы каталогов Active Directory.

Третья часть раздела посвящена практическим вопросам управления системой безопасности корпоративной сети — учетными записями пользователей, компьютеров, групп, организационными подразделениями. Описан также механизм групповых политик — мощное средство управлением настройками пользовательской среды и параметров компьютеров в большой корпоративной сети.

В четвертой части описаны технологии управления сетевой безопасностью — протокол аутентификации Kerberos и применение шаблонов безопасности для настройки параметров безопасности серверов и рабочих станций.

Задачи сетевого администратора при управлении инфраструктурой службы каталогов:

* планирование и реализация пространства доменных имен компании или организации для службы каталогов Active Directory;
* планирование и реализация IP-сетей и сайтов AD для управления процессами репликации контроллеров домена и аутентификации пользователей в сети;
* планирование и размещение в сети контроллеров домена, выполняющих функции хозяев операций;
* планирование и реализация правил создания и именования учетных записей пользователей, компьютеров и групп;
* планирование и реализация стратегии использования групп для управления доступом к сетевым ресурсам;
* планирование и реализация иерархии организационных подразделений для делегирования административных полномочий и применения групповых политик;
* планирование и разработка набора групповых политик для управления рабочей средой пользователей и параметров компьютеров;
* проведение анализа сетевой безопасности, настройка требуемого уровня сетевой безопасности на серверах и рабочих станциях.