Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**
**(ФГБОУ ВО «АмГУ»)**

# АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

сборник учебно-методических материалов

для направления подготовки 10.03.01 Информационная безопасность

Благовещенск, 2019

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
Университета

Составитель: Тодосейчук А.А.
Администрирование информационных систем: сборник учебно-методических материалов для направления подготовки 10.03.01 Информационная безопасность – Благовещенск: Амурский гос. ун-т, 2019.

© Амурский государственный университет, 2019
© Кафедра Информационных и управляющих систем, 2019
© Тодосейчук А.А., составление

**1. Краткое изложение лекционного материала**

1. Информационные системы

Информационная система - по законодательству РФ - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Судя по определению из Википедии – достаточно большой энциклопедии.:

Информационная система (ИС) — это система, в которой присутствуют информационные процессы (хранение, передача, преобразование информации). ИС, получая информацию, преобразует ее в информационный продукт.

·АСУ — Автоматизированные системы управления

АСУ П — Автоматизированные системы управления предприятия

АСУ ТП — Автоматизированные системы управления технологическими процессами

ИУС — Информационно-управляющие системы

ИИС — Информационно-измерительные системы

ИПС — Информационно-поисковые системы

ИСС — Информационно-справочные системы;

ГИС — Геоинформационные системы

СИИ — Системы искусственного интеллекта

САПР — Системы автоматизации проектной деятельности

СПД — Системы передачи данных

ИИС- Интеллектуальные информационные системы

2. **Общие положения Администрирования информационных систем**

А. Создание Правил эксплуатации и назначение ответственных за их соблюдение

Цель: Обеспечение правильной и надежной работы информационных систем.

Часть 1: Необходимо определить обязанности и процедуры по администрированию и обеспечению функционирования компьютеров и сетей. Они должны быть зафиксированы в инструкциях и процедурах реагирования на инциденты. Для уменьшения риска некорректных или несанкционированных действий следует применять принцип разделения обязанностей.

Часть 2: Аудиторы должны проверить наличие правил по эксплуатации, разработке, сопровождению, тестированию, убедиться, что все необходимые операции должным образом документированы.

Б. Проектирование информационных систем и их приемка

Цель: Свести риск отказов информационных систем к минимуму.

Часть 1: Для обеспечения доступности ресурсов и необходимой производительности информационных систем требуется предварительное планирование и подготовка. Для уменьшения риска перегрузки систем необходимо оценить будущие потребности и необходимую производительность. Эксплуатационные требования к новым системам следует определить, документировать и проверить до их приемки. Должны быть выработаны требования к переходу на аварийный режим для сервисов, поддерживающих несколько приложений.

Часть 2: Аудиторы должны проверить критерии приемки информационных систем, оценки их производительности, планы восстановительных работ по каждому сервису.

В. Защита от вредоносного программного обеспечения

Цель: Обеспечить целостность данных и программ

Часть 1: Для предотвращения и выявления случаев внедрения вредоносного программного обеспечения требуется принятие соответствующих мер предосторожности. В настоящее время существует целый ряд вредоносных программ ("компьютерные вирусы", "сетевые черви", "Троянские кони" и "логические бомбы"), которые используют уязвимость программного обеспечения по отношению к несанкционированной модификации. Администраторы информационных систем должны быть всегда готовы к проникновению вредоносного программного обеспечения в информационные системы и принимать специальные меры по предотвращению или обнаружению его

внедрения. В частности, важно принять меры предосторожности для предотвращения и обнаружения компьютерных вирусов на персональных компьютерах.

Часть 2: Аудиторы должны убедиться, что процедуры, препятствующие внедрению вредоносного программного обеспечения, должным образом документированы, приняты адекватные меры предосторожности, случаи заражения регистрируются.

Г. Обслуживание систем

Цель: Обеспечить целостность и доступность информационных сервисов.

Часть 1: Для поддержания целостности и доступности сервисов требуется выполнение некоторых служебных процедур. Должны быть сформированы стандартные процедуры резервного копирования, регистрации событий и сбоев, а также контроля условий функционирования оборудования.

Часть 2: Аудиторы должны убедиться, что процедуры резервного копирования соответствуют требованиям организации, операторы ведут протоколы всех производимых операций, неисправности регистрируются и принимаются меры к их устранению.

Д. Сетевое администрирование

Цель: Обеспечить защиту информации в сетях.

Часть 1: Управление безопасностью сетей, отдельные сегменты которых находятся за пределами организации, требует особого внимания. Для защиты конфиденциальных данных, передаваемых по открытым сетям, могут потребоваться специальные меры.

Часть 2: Аудиторы должны проверить защитные меры, применяемые в организации.

Е. Защита носителей информации

Цель: Предотвратить повреждение информационных ресурсов и перебои в работе организации.

Часть 1: Необходимо контролировать носители информации и обеспечивать их физическую защиту. Следует определить процедуры для защиты носителей информации (магнитные ленты, диски, кассеты), входных/выходных данных и системной документации от повреждения, хищения и несанкционированного доступа.

Часть 2: Аудиторы должны проверить установленные процедуры контроля, режим хранения носителей информации.

Ж. Обмен данными и программным обеспечением

Цель: Предотвратить потери, модификацию и несанкционированное использование данных.

Часть 1: Обмены данными и программами между организациями необходимо осуществлять на основе формальных соглашений. Должны быть установлены процедуры и стандарты для защиты носителей информации во время их транспортировки. Необходимо уделять внимание обеспечению безопасности при использовании электронного обмена данными и сообщениями электронной почты.

Часть 2: Аудиторы должны проверить существующие меры защиты электронного обмена данными, меры ИБ внутреннего электронного документооборота.

Администрирование ИС будем рассматривать на примере информационных сетей, серверных операционных систем и систем управления БД.

З. Работа с пользователями.

Цель: управление пользовательскими бюджетами.

Сюда входит создание и удаление пользовательских бюджетов (учетных записей), их блокировка и разблокирование, настройка сценариев входа, консультирование пользователей по различным аспектам работы с системой и нахождению тех или иных ресурсов.

И. Анализ производительности и оптимизация системы.

Цель: Оптимальное реагирование на инцидент

Большинство систем имеют оптимальные настройки "по умолчанию" и не требуют особого вмешательства. Однако, узкие места все же могут возникать. Производители известных сетевых операционных систем на основе богатого опыта эксплуатации выводят наборы эмпирических правил, помогающих администратору вносить изменения в настройки с минимальным риском ухудшить другие показатели или сделать систему неработоспособной. Такие рекомендации имеются, в

частности, у фирм Novell и Sun Microsystems; администратору остается только их изучить и знать перечень параметров, которые необходимо контролировать. Многих проблем можно избежать еще на стадии планирования сети. В частности, неправильный выбор типов кадров Ethernet и их соотношения может привести к резкому снижению производительности, а то и к нарушению работы системы при отключении одного из компонентов.

К. Учет системных ресурсов и модернизация.

Цель: обнаружение тенденций к появлению узких мест в системе и устранение их.

Учет ресурсов позволяет заметить тенденции к появлению узких мест до того, как появятся проблемы с производительностью и провести соответствующую модернизацию. Кроме того, система учета совершенно необходима при платном использовании ресурсов. Сюда относится контроль использования дискового пространства, печати, учет трафика.

Л. Аудит

Данные используются почти всеми приведенными выше задачами. С целью обеспечения непротиворечивости получаемой информации доступ к подсистеме аудита должен быть ограничен. Причем лицо, ответственное за подсистему аудита не должно иметь административных полномочий по управлению системой и данным, по которым аудит ведется. Такое разделение позволит существенно повысить уровень безопасности: если человек знает, что его действия протоколируются, то он воздержится от попыток совершения каких-либо манипуляций с информацией во вред компании. По этой же причине он оказывается защищенным от давления со стороны третьих лиц совершить нечто противоправное.

Документация

Все аспекты деятельности всех администраторов должны быть обеспечены нормативными и методическими документами. Это защитит как интересы руководства компании, так и администраторов. Кроме того, как показывает опыт, наличие типовых инструкций позволяет четче и слаженней действовать в нестандартных ситуациях. Состав пакета нормативных документов может быть примерно следующим:

1. Положение о локальной сети компании.
2. Инструкция администратору серверов.
3. Инструкция администратору баз данных.
4. Инструкция пользователю.
5. Инструкция администратору информационной безопасности.
6. Инструкция аудитору.
7. Процедура оформления доступа к ресурсам.
8. Инструкция по резервному копированию и восстановлению информации.
9. Инструкция по антивирусной безопасности.
10. Инструкция о парольной защите.

Информационная политика компании

Итак, основное назначение информационной политики представить действенный инструмент и правила, согласно которым сотрудники компании могут оценить важность вверенной им информации, смогут смело использовать ее в собственных интересах и интересах компании. При этом риск навредить основной деятельности компании должен сохраняться минимальным. Фактически, должен соблюдаться врачебный принцип «не навреди». Однако надо иметь в виду, что отсутствие вразумительной информации может также вредить деятельности и развитию компании, так же как и ее переизбыток. Все должно быть в меру.

Информационная политика, это своего рода шкала (линейка), или несколько шкал, по которым человек может измерить и оценить информацию, которой он владеет. А далее, «примерив» полученные результаты на поставленную задачу, принимается окончательное решение использовать или нет, публиковать или нет. Особенно частое заблуждение, что на некоторых мерках, сотрудники, которые разрабатывают информационную политику, забывают ставить контрольные даты. Очень опасное заболевание.

Информация должна быть актуальной. Чтобы это увидеть, «погуляйте» по Интернету, и Вы найдете очень большое количество подтверждений отсутствия контрольных точек в информаци-

онной политике той или иной фирмы. Самое распространенное явление, на сайтах компаний часто представлена информация 2-3 годичной давности. И дело здесь как раз в отсутствии либо информационной политики как таковой, либо отсутствие контрольных временных точек.

Если у Вас система построена так, что она умеет реагировать на запланированные события, то соответственно, Вы всегда будете владеть актуальной и ценной для публикации (и не только) информацией.

Классификаторы информации

Давайте проанализируем возможные информационные классификаторы, которые собственно, и определяют информационную политику.

Прежде всего, степень открытости информации: конфиденциальная, доступная только узкому кругу лиц. Для служебного пользования информация доступна всем (или почти всем) сотрудникам компании, но не предназначенная для открытой публикации. И публичная информация, которая доступна всему мировому сообществу. Есть, правда, еще один параметр – устаревшая информация, фактически она доступна всем, но она уже неинтересна. Публикация такой информации может принести как пользу, так и вред компании. С ней надо обращаться осторожно и в зависимости от ситуации.

Вот мы добрались до следующего классификатора. А именно стоимость информации относительно основной деятельности компании. Со временем стоимость информации падет. Это естественный процесс, такой же, как само старение человека, приводит либо к отмиранию информации, либо к понижению ее социального статуса.

Конечно, можно говорить о том, что любая устаревшая информация имеет более низкий социальный статус (в конце концов, становится публичной), но это не всегда так. Пример, многочисленные правительственные закрытые архивы. Информация, скажем столетней давности, далеко уже не так ценна, как изначально. Но мы не можем даже предположить, к каким социальным последствиям может привести ее публикация. То есть, стоимость такой информации сложно определить. Тогда в силу того же медицинского принципа «не навреди», мы ее не публикуем.

Компьютерные сети

Под компьютерной сетью понимается совокупность компьютеров, связанных коммуникационной системой и снабженных необходимым программным обеспечением, позволяющим пользователям и приложениям получать доступ к ресурсам компьютеров.

В последнее время наблюдается быстрый рост числа сетей, подключенных к сообществу компьютерных сетей Internet. Темпы этого роста носят экспоненциальный характер. Популярность Internet определяется наличием простого в использовании программного обеспечения, отработанной технологии межсетевого обмена и большого количества информационных материалов.

В рамках этой темы можно выделить несколько основных проблем, с которыми сталкивается администратор информационной сети:

- Организация сети TCP/IP;
- Подключение локальной или корпоративной сети к Internet;
- Определение и управление маршрутами передачи информации в этой сети, или, другими словами, проблема маршрутизации;
- Получение доменного имени для организации, т.к. запомнить числовые адреса задача трудная и, с учетом числа машин в сети, не выполнимая. По вашему доменному имени всегда пользователи смогут добраться до информационных ресурсов вашей организации;
- Обмен электронной почтой как внутри организации, так и с адресатами за ее пределами;
- Организация информационного обслуживания на базе технологий Internet, плавно перетекающая в технологию Intranet;
- Проблема безопасности сети TCP/IP.

Остановимся на каждом из этих направлений деятельности администратора системы или группы администраторов более подробно.

Организация сети TCP/IP

Прежде, чем организовывать сеть TCP/IP следует достаточно хорошо разбираться в принципах ее функционирования. В отличии от многих других сетей, в TCP/IP практически на каждой

машине следует иметь массу информации необходимой для ее настройки, которая по сети не передается. В этом есть как свои преимущества, так и свои недостатки.

Недостатки сводятся к довольно большой ручной работе по настройке каждой машины, каждого сетевого интерфейса. При этом предварительно должна быть продумана топология сети, ее физическая и логическая схемы, определено оборудование.

После того как физическая сеть собрана, администратор должен собственноручно назначить на каждой машине адреса интерфейсам. Обычно это делается с консоли того компьютера, который настраивается для работы в сети. В последнее время появилась возможность динамической настройки с одного рабочего места всех машин сети. Однако, как и в любом деле, кроме явных преимуществ есть и скрытые недостатки такого подхода. Главный из них - это учет статистики работы с каждой из машин системы. При динамическом назначении адресов машина может в разное время получать разные адреса, что не позволяет по адресу проидентифицировать машину. Многие же системы анализа трафика основываются на том, что соответствие между адресом и компьютером неизменно. Именно на этом принципе построены многие системы защиты от несанкционированного доступа.

Подключение локальной или корпоративной сети к Internet

Подключение локальной сети TCP/IP к Internet осуществляется через местного провайдера. Обычно это та же организация, у которой был получен блок адресов для WEB сервера.

Администратор локальной сети должен определить маршрутизатор – устройство, которое распознают массу различных протоколов и способны правильно направлять пакеты информации из одной сети в другую. Стоит маршрутизатор достаточно много. Если подключаемая сеть большая и требуется мощное устройство для обслуживания ее внешнего трафика, то приобретение маршрутизатора оправдано, если же сеть небольшая, то можно обойтись персональным компьютером, на который следует установить соответствующее программное обеспечение.

Маршрутизация в сетях TCP/IP

До тех пор пока вся локальная сеть представляет из себя простой сегмент сети Ethernet, не возникает проблем с приемом и передачей сообщений в рамках этой сети. Однако стоит разбить сеть на несколько сегментов и установить шлюзы между ними, как сразу возникает проблема маршрутизации сообщений в этой сети.

Основа маршрутизации - это таблица маршрутов на каждом из компьютеров в сети и правила изменения этой таблицы в случае изменения состояния самой сети.

Маршрутизация - это средство не только прокладки маршрутов, но и средство блокирования маршрутов пересылки пакетов по сети. Если таблицы настроены неправильно, то в лучшем случае пакеты будут доставляться медленно, а в худшем случае они будут доставляться не туда куда следует, что может привести к нарушению безопасности сети передачи данных. Очень часто средства маршрутизации используют для атак на системы, включенные в Internet. Известны, так называемые, ICMP-штормы, когда пакеты определенного вида могут блокировать прием/передачу информации по сети.

Если администратор по тем или иным причинам должен закрыть часть своей сети от доступа с других машин Internet, то в этом случае также можно использовать таблицу маршрутов, удаляя из нее определенные пути, или блокируя их другими средствами контроля сетевого трафика.

Система доменных имен

Система доменных имен занимает одно из центральных мест среди информационных сервисов Internet. Это место столь велико, что часто пользователи сети отождествляют ошибки при работе системы доменных имен с ошибками работы самой сети, действительно, большинство информационных ресурсов сети пользователям известны по их доменным именам.

Для организации больших сетей или виртуальных сетей через Internet, доменные имена становятся необходимыми и проблема управления этими адресами ложится на плечи администратора сети.

Сервис доменных имен допускает и разделенное управление поддоменами. Особенно это актуально для сетей, имеющих распределенную структуру. Очень трудно из одного места уследить за всем, что может твориться в филиале за сотни километров, гораздо проще часть прав по управ-

лению удаленной частью сети возложить на местную администрацию. В этом случае происходит делегирование управления поддоменом.

Администрирование электронной почты

То, как организация оперирует электронной почтой, также важно, как и использование системы. Правила безопасности и инструкции при подходящем случае становятся темой судебных процессов, основанием для жалоб и прочих хлопот, которые мешают работе организации или пользователей.

Другие аспекты работы с электронной почтой, будь то содержание посланий или их обработка, обычно не воспринимаются серьезно. А они являются реальными вопросами, так как находят порой отражение в скандальных делах и проблемах, связанных с электронной почтой и отражающихся на безопасности организации. Правила безопасности электронной почты должны устанавливать определенные обязанности и для пользователя, и для администратора. Если организация пользуется внешними услугами для обеспечения работы электронной почты, то следует проверить контракт, чтобы убедиться, что провайдер услуг управляет системами электронной почты в соответствии с принятыми в организации правилами.

Самое распространенное приложение Internet может оказаться и самым опасным. Электронная почта может использоваться для пересылки секретных данных, оскорблений и создавать проблемы для службы безопасности. Все проблемы можно решить, если организация контролирует трафик электронной почты и содержимое посланий, а также архивирует сообщения, чтобы в будущем можно было разобраться в возникшей проблеме.

Организация информационного обслуживания на основе технологий Internet

В последнее время все чаще стали говорить об Intranet. При этом обычно понимают использование информационных технологий Internet для создания информационных систем внутри организации.

Исходя из этого, концепция администрирования сетей TCP/IP расширяется администрированием серверов World Wide Web и настройкой этих серверов для работы с разными клиентами, условной генерацией ответов в зависимости от типа клиента, адреса машины и кодировки (языка).

При использовании World Wide Web для нужд организации обычно рассматривается два направления работ:

- размещение рекламы и другой информации для пользователей Internet;
- организация тематических интерфейсов для доступа к ресурсам сети для работников организации.

Кроме World Wide Web при работе с Internet используют и другие информационные технологии. FTP-архивы - для внутреннего использования FTP-архив также чрезвычайно полезен, т.к. может использоваться в качестве основного центрального депозитария материалов и программного обеспечения организации.

А также Режим удаленного терминала продолжает оставаться одним и главных способов первичной организации доступа к локальным информационным системам через сеть. Такое использование системы позволяет отказаться от копирования системы на каждый из компьютеров пользователей и централизованное управление информационным ресурсом.

Проблемы безопасности сетей TCP/IP

При всех своих достоинствах сети TCP/IP имеют один врожденный недостаток - отсутствие встроенных способов защиты информации от несанкционированного доступа. Дело в том, что информация при таком способе доступа как удаленный терминал, передается по сети открыто. Это означает, что если некто найдет способ просмотреть передаваемые по сети пакеты, то он может получить коллекцию идентификаторов и паролей пользователей TCP/IP сети. Способов совершить такое действие огромное множество. Аналогичные проблемы возникают и при организации доступа к архивам FTP и серверам World Wide Web. Поэтому одним из основных принципов администрирования TCP/IP сетей является выработка общей политики безопасности, которая заключается в том, что администратор определяет правила типа "кто, куда и откуда имеет право использовать те или иные информационные ресурсы".

Управление безопасностью начинается с управления таблицей маршрутов. При статическом администрировании маршрутов включение и удаление последних производится вручную, в случае динамической маршрутизации эту работу выполняют программы поддержки динамической маршрутизации.

Следующий этап - это управление системой доменных имен и определение разрешений на копирование описания домена и контроля запросов на получение IP-адресов. Нашумевшая история с сервером InfoArt - это типичная атака на этот вид информационного сервиса Internet.

Следующий барьер - это системы фильтрации TCP/IP трафика. Наиболее распространенным средством такой борьбы являются системы FireWall (межсетевые фильтры или, в просторечье, "стены"). Используя эти программы можно определить номер протокола и номер порта, по которым можно принимать пакеты с определенных адресов и отправлять пакеты на также определенные адреса. Одним из нетипичных способов использования этого типа систем являются компьютерные сетевые игры, например, F-19. "Стена" позволяет поражать противника, т.к. пропускает ваши пакеты, и быть одновременно неуязвимым для противника, т.к. его пакеты отфильтровываются системой.

И, наконец, последнее средство защиты - это шифрация трафика. Для этой цели также используется масса программного обеспечения, разработанного для организации защищенного обмена через общественные сети.

Администрирование информационных сетей

Основные понятия

- Информационно вычислительная сеть (ИВС) – комплекс программных и аппаратных средств для обеспечения автоматизации производства и других сфер деятельности человека, включающий в качестве составной части кабельное и сетеобразующее оборудование.
- Администратор ИВС – должностное лицо, ответственное за работоспособность и надлежащее функционирование всех частей ИВС.
- Пользователь ИВС (Юзер) - физическое лицо, имеющее доступ к определенным ресурсам ИВС, идентифицируемое бюджетом пользователя(учетной записью). Администратор ИВС так же является пользователем ИВС, обладая, в общем случае, неограниченным доступом ко всем ресурсам ИВС.
- Бюджет или учетная запись пользователя(Аккаунт) – запись в специализированной БД (БД учетных записей), содержащая информацию о пользователе ИВС. Используется для идентификации пользователя в системе, проверке полномочий пользователя и обеспечения доступа пользователя к тем или иным ресурсам системы. Характеризуется атрибутами, например имя для входа(логин), пароль, профиль в системе, список принадлежности к группам и т.п. Пароль служит для защиты бюджета от несанкционированного использования.
- Регистрация пользователя в системе – создание администратором ИВС (или другим уполномоченным лицом) бюджета пользователя для конкретного физического лица.
- Ресурсы ИВС – физические и логические объекты ИВС, имеющие определенную функциональность, доступную для использования.
- Права доступа к ресурсу – степень свободы действий пользователя по отношению к данному ресурсу.
- Назначение прав доступа к ресурсу – процедура создания в системе специальной записи пользователя или ее аналогу(например группа пользователей) присваиваются определенные права доступа к ресурсу. Назначение прав доступа в современных ИВС осуществляется через списки управления доступом (Access Control List-ACL)
- Список управления доступом (ACL) – хранилище в виде отдельных записей, с информацией о том, кто обладает правами на ресурс и каковы эти правила.
- Аудит или контроль использования ресурсов – процесс контроля использования ресурсов, включающий возможность ведения журнала попыток доступа к ресурсам. Журнал аудита ведется на основе данных, поступающих от процедур авторизации.

Авторизация, аутентификация, идентификация и аудит

• Идентификация - процедура распознавания субъекта по его уникальному идентификатору, присвоенному данному субъекту ранее и занесенному в базу данных в момент регистрации субъекта в качестве легального пользователя системы.

• Аутентификация - процедура проверки подлинности входящего в систему объекта, предъявившего свой идентификатор. В зависимости от степени доверительных отношений, структуры, особенностей сети и удаленностью объекта проверка может быть односторонней или взаимной. В большинстве случаев она состоит в процедуре обмена между входящим в систему объектом и ресурсом, отвечающим за принятие решения ("да" или "нет"). Данная проверка, как правило, производится с применением криптографических преобразований, которые нужны, с одной стороны, для того, чтобы достоверно убедиться в том, что субъект является тем, за кого себя выдает, с другой стороны - для защиты трафика обмена субъект-система от злоумышленника. Таким образом, идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности пользователей. Именно от корректности решения этих двух задач (распознавания и проверки подлинности) зависит, можно ли разрешить доступ к ресурсам системы конкретному пользователю, т.е. будет ли он авторизован.

• Авторизация - процедура предоставления субъекту определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к её ресурсам.

Технологии идентификации

В последнее десятилетие интенсивно развивается направление электронной идентификации, в которой сбор информации происходит с минимальным участием человека. Это объясняется тем, что оператор может допустить ошибку при вводе данных, например, с клавиатуры компьютера. Технологии автоматической идентификации наиболее полно соответствуют требованиям компьютерных систем и систем управления, где нужно четко распознавать объекты в реальном масштабе времени. Кратко рассмотрим основные технологии. Заметим, что на практике часто они используются в различных комбинациях.

Штрих - кодовая идентификация

Штрих-коды в основном используются производителями товаров для автоматизации товародвижения. В настоящее время штриховые коды EAN/UPC лежат в основе всемирной многоотраслевой коммуникационной системы, развитие которой обеспечивается двумя крупнейшими специализированными международными организациями –EAN(European Article Number) International и AIM(Autimation Identification) International. Наиболее широко распространен тринадцатиразрядный код EAN-13, разработанный в 1976г. для удовлетворения требований пищевой промышленности на базе кода UPC (Universal Product Code), введенного в США еще в 1973г.

Штриховой Код EAN13 является непрерывным, имеет фиксированную длину и высокую плотность записи позволяет отобразить 13 цифр от 0 до 9.


Рис.1. Пример штрихового кода EAN

Кодовое обозначение может выражаться восемью (EAN8) или тринадцатью (EAN13) цифрами, причем во втором случае реально кодируется только двеннадцать цифр. Знаки штрихового Кода EAN состоят из двух штрихов и двух промежутков.

Штриховое изображение всех 12-ти (8-ми) цифр составляет в целом символ кода EAN.

Краевые знаки (удлиненные штрихи - знаки начала и конца символа) определяют его границы; делится символ на две части разделительным знаком (удлиненные штрихи в центре символа),

К достоинствам применения штрих-кодовой идентификации относятся:

· максимальное снижение бумажного документооборота и количества ошибок при вводе информации;

· повышение скорости обслуживания клиентов;

· автоматизация основных технологических процессов товародвижения на всех этапах от производителя до конечного покупателя.

Основные недостаткам штрих-кодовой идентификации:

· данные идентификационной метки не могут дополняться - штриховой код записывается только один раз при его печати;

· небольшой объем данных (обычно не более 50 байт); (??Сколько это символов?)

· данные на метку заносятся медленно - для получения штрихового кода обычно требуется напечатать его символ либо на упаковке, либо на бумажной этикетке, а наклеивание липкой этикетки часто выполняется вручную;

· данные на метке представлены в открытом виде и не защищают товары от подделок и краж;

· штрих-кодовые метки недолговечны, т.к. не защищены от пыли, сырости, грязи, механических воздействий.

В настоящее время штрих-кодовая идентификация начинает вытесняться технологией радиочастотной идентификации.

Радиочастотная идентификация

В средствах радиочастотной идентификации (RFID - Radio Frequency Identification Device) разработчики постарались развить все достоинства штрих-кодовой идентификации и преодолеть практически все недостатки и ограничения. В настоящее время данная технология интенсивно внедряется во многие отрасли мирового хозяйства. RFID позволяет получать информацию о предмете без прямого контакта. Дистанции, на которых может происходить считывание и запись информации, могут варьироваться от нескольких миллиметров до нескольких метров в зависимости от используемых технологий (главным образом, от несущей частоты, находящейся в пределах от 125 кГц до 5,8 ГГц). Большинство применяемых для идентификации сотрудников корпораций смарт-карт с применением компонент производства Ангстрем, HID, Atmel, Mifare, EM Microelectronic Marin, Microchip и др. чаще всего используют несущие частоты 125 кГц или 13,56МГц.

EM4100 (EM4102, EM-Marin) - формат бесконтактных радиочастотных идентификационных карт компании EM Microelectronic-Marin, одни из самых распространённых в России.

Mifare — торговая марка семейства бесконтактных смарт-карт. Торговая марка объединяет несколько типов микросхем смарткарт, микросхемы считывателей и продукты на их основе. Владельцем торговой марки является NXP Semiconductors.

Считается наиболее распространённой торговой маркой бесконтактных смарт-карт в мире: продано более 1 млрд смарт-карт и 10 млн считывателей.

Биометрическая идентификация

Данная технология основана на применении статистического анализа биологических наблюдений и явлений. Биометрическая характеристика - это измеримая физиологическая или поведенческая черта человека.

Биометрические характеристики можно разделить на две группы:

1 Физиологические биометрические характеристики (называемые физическими или статическими) - характеристики, основанные на данных, полученных путём измерения анатомических данных человека(отпечатки пальцев, форма лица, кисти, структура сетчатки глаза и др.).

2 Поведенческие биометрические характеристики (также называемые динамическими биометрическими характеристиками) - биометрические характеристики, основанные на данных, полученных путём измерения действий человека. Характерной чертой для поведенческих характеристик является их протяжённость во времени (типичные примеры - голос, подпись).

Биометрические системы отличаются, в основном, объектами и способами измерений. Пользователь посредством регистрирующего устройства (например, сканера или камеры) предоставляет системе образец - опознаваемое, необработанное изображение или запись физиологической или поведенческой характеристики. Биометрический образец обрабатывается для получения информации об отличительных признаках, в результате чего получается ЭИП (эталонный идентификатор пользователя или эталон для проверки). ЭИП представляет собой числовую последова-

тельность, при этом сам образец невозможно восстановить из эталона. Снятая в процессе идентификации характеристика сравнивается с ЭИП. Поскольку эти два значения (полученное при попытке доступа и ЭИП) полностью никогда не совпадают, то для принятия положительного решения о доступе степень совпадения должна превышать определенную настраиваемую пороговую величину. При этом эффективность биометрических систем характеризуется коэффициентом ошибочных отказов и коэффициентом ошибочных подтверждений.

Статья по английскому, по созданию отпечатка действия или мыслей при воздействии на человека.

Идентификации на основе карт с магнитной полосой

Карты с магнитной полосой уже более двух десятилетий используются в системах контроля физического доступа. Магнитные карты срабатывают при проведении в определенном направлении и с определенной скоростью по щели считывателя. Повременные магнитные полосы изготовлены из материалов, требующих сильных магнитных полей для записи и уничтожения информации, с целью сохранности информации от случайного размагничивания.

Существенным преимуществом магнитных карт является их низкая стоимость. К основным недостаткам данной технологии можно отнести:

- ограничение по объему информации, которая может быть записана на магнитную полосу;
- незащищенность от копирования;
- чувствительность к загрязнению, механическим повреждениям (например, царапинам, изломам), воздействию влаги;
- короткий срок службы (не более 3 лет).

Технологии аутентификации

Для того чтобы понять, что такое AAA и, в частности, аутентификация, обратимся к простому примеру: Ваш сотовый телефон. Телефон - это устройство, куда для начала работы Вы вкладываете SIM-карту. При включении сотового от Вас требуют ввода пин кода. После правильного ввода PIN-кода (как правило, это 4 легко запоминаемые цифры) телефон начинает работать.

Налицо так называемая двухфакторная аутентификация. Вам надо иметь персональный носитель (SIM-карту) и знать личный PIN-код. Они связаны между собой. Аналогом SIM-карты может являться микропроцессорная смарт-карта или устройство eToken, к которому привязан личный PIN-код. Только в отличие от сотового телефона PIN-код для доступа к информационной системе предприятия содержит, как правило, не менее 5-7 символов различных регистров (не только цифр). Да и алгоритмы аутентификации и шифрования там намного сложнее, чем используемые в сотовой связи A3 (алгоритм аутентификации), A8 (алгоритм генерации криптоключа), A5/2 (алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров).

A3 - Алгоритм аутентификации абонента в сети мобильной связи стандарта GSM.

A8 - Алгоритм генерации сеансового ключа для шифра A5

A5 - Потоковый шифр с 64-битовым ключом (эффективная длина составляет 54 бита), используемый в сетях мобильной связи стандарта GSM для защиты трафика, передаваемого между мобильным терминалом и базовой станцией. Подвержен криптоанализу «в реальном времени», признан ненадёжным.

В настоящее время в качестве реализации A3/A8 используется алгоритм хэш-функции COMP128 - Алгоритм хэш-функции с 256-битовым вводом и 128-битовым выводом.

Рассмотрим основные методы аутентификации по принципу нарастающей сложности. Начнем с самого простого и общеизвестного метода - аутентификация по паролю. Поскольку данная технология, как правило, используется без изменения параметров в течение длительного времени (неделя, месяц, год - в зависимости от политик безопасности предприятия), то она получила название "аутентификация по многоразовым паролям".

Аутентификация по многоразовым паролям

Учетные записи пользователей современных операционных систем включают в себя службу аутентификации, которая может хранить простейший идентификатор (login) и пароль (password) пользователя в своей базе данных. При попытке логического входа в сеть пользователь

набирает свой пароль, который поступает в службу аутентификации. По итогам сравнения пары login/password с эталонным значением из базы данных учетных записей пользователей пользователь может успешно пройти процедуру простейшей аутентификации и авторизоваться в информационной системе. В зависимости от степени защищенности в рамках эволюционного развития операционных систем Windows компанией Microsoft использовались протоколы LAN Manager (LM), NT LAN Manager (NTLM), NT LAN Manager версии 2 (NTLM v2) и Kerberos. В качестве примера кратко рассмотрим Kerberos, как наиболее распространенный и защищенный на сегодняшний день протокол аутентификации в локальных сетях.

Задачи протокола

Протокол аутентификации должен выполнять по крайней мере две задачи. Во-первых, он должен безопасно передавать транзакции от запросчика в базу данных аутентификации и на любой другой компьютер, на котором размещен соответствующий ресурс. Во-вторых, он должен безопасно и надежно хранить пароль или маркер. Последнее представляет особый интерес для взломщиков паролей. Протокол аутентификации должен защитить введенную пользователем информацию при пересылке в базу данных аутентификации (т. е. SAM или AD). Для этого протокол подписывает, скрывает или шифрует транзакцию. Кроме того, ей присваивается временная метка, чтобы взломщик не мог воспользоваться учетными данными в будущем. Чтобы не позволить немедленно извлечь пароль пользователя из базы данных, протокол должен обеспечить скрытное хранение паролей в базе данных аутентификации.

В течение более чем десяти лет протоколы аутентификации в основном обеспечивали защиту путем сохранения паролей в скрытой форме (обычно хешированной) в базе данных аутентификации и полного запрета на передачу паролей между запросчиком и базой данных аутентификации простым текстом (даже в скрытой форме). Процесс запрос—ответ выглядит следующим образом:

1 Компьютер получает данные для идентификации и аутентификации от пользователя и запрашивает аутентификацию на соответствующем сервере.

2 Сервер аутентификации генерирует случайное произвольное значение (называемое запросом - challenge) и посылает его запросчику.

3 Запросчик получает запрос и производит над ним и скрытой формой пароля математические операции, а затем передает результат (называемый ответом - response) серверу аутентификации.

4 Сервер аутентификации также выполняет математические манипуляции с запросом методом, идентичным используемому на рабочей станции, и сравнивает результат с полученным ответом. Если результаты совпадают, то запросчик считается успешно аутентифицированным.

В протоколах аутентификации используется процесс запрос—ответ, поэтому пароль никогда не передается через сеть.

LAN Manager появился во времена DOS и продолжал использоваться с первыми версиями Windows. NTLM был выпущен вместе с NT. Новшеством пакета обновлений NT Server 4.0 Service Pack 4 (SP4) стал NTLMv2, а Windows 2000 привнесла Kerberos. По умолчанию все компьютеры с Windows 2000 и более новыми операционными системами совместимы со всеми четырьмя протоколами аутентификации. Передавая в эти системы соответствующие команды, другие рабочие станции и серверы могут выбирать протокол для обработки запроса аутентификации. Системы Windows 9x и более поздние с полным набором программных исправлений совместимы с LM, NTLM и NTLMv2. На платформе Microsoft Kerberos может использоваться только клиентами Windows 2000 (или более новыми) при обращениях в домены Windows 2000 (и выше). Компьютер с Windows 2000 или более новой версией операционной системы должен иметь Kerberos и по крайней мере еще один из протоколов аутентификации.

Исследования в области безопасности показали, что более старые протоколы (LM и NTLM) уязвимы в случае прослушивания и атак с разгадыванием пароля.

Поэтому, если возможно, рекомендуется использовать только Kerberos и NTLMv2. Чтобы убедиться в правильности этого совета, следует оценить возможности каждого протокола.

LAN Manager

Компания IBM разработала протокол LAN Manager, применив его в ранних версиях Windows и сетях Windows. Как все протоколы аутентификации Microsoft, LAN Manager генерирует хеш паролей (LM hash), который хранится и используется отправителем и получателем в процессе аутентификации. LAN Manager формирует LM-хеши, изменяя все буквы пароля на верхний регистр, разбивая пароль на две 7-символьные половины, а затем шифруя. В дальнейшем LM-хеш используется в нескольких последовательных операциях, аналогичных процессу запрос—ответ, описанному выше. Если раньше LAN Manager был вполне приемлем, то сейчас он считается очень ненадежным. С помощью специальных инструментов пароли, зашифрованные методом хеширования LAN Manager, можно всего за несколько секунд преобразовать в простой текст. LM-хешам свойственны принципиальные недостатки, а также имеется ряд уязвимых мест:

- ❖ пароли могут состоять из ограниченной последовательности 128 символов ASCII;
- ❖ длина пароля не превышает 14 символов;
- ❖ если пароль содержит менее 14 символов, то отсутствующие символы заменяются легко угадываемой хешированной формой, что позволяет точно определить длину пароля;
- ❖ перед кэшированием LAN Manager преобразует все буквенные символы пароля в верхний регистр.

Почему LAN Manager до сих пор не вышел из употребления? В целях обратной совместимости он активен по умолчанию во всех компьютерах Windows, в том числе Windows Server 2003. В новейших базах данных аутентификации Windows слабый LM-хеш хранится наряду с более надежными просто на случай, если придется выполнить транзакцию LAN Manager. Если на предприятии не используются другие приложения, требующие аутентификации LAN Manager, то можно (и нужно) LAN Manager отключить.

NTLM

С появлением NT компания Microsoft спроектировала и развернула более надежный протокол аутентификации NTLM. В NTLM используется более эффективный алгоритм аутентификации, который создает более надежный хеш паролей (NTLM hash). Пароль NTLM может содержать до 128 символов. В отличие от хеширования LAN Manager, ограниченного использованием только символов ASCII, NTLM совместим с полным набором символов Unicode, что повышает сложность паролей. NTLM-хеш отсекается на 128-м символе, преобразуется в 16-разрядное значение Unicode, обрабатывается распределительной функцией MD4 и сохраняется в 32-символьной шестнадцатеричной строке. За счет использования NTLM-хеша в операциях запрос—ответ последовательность аутентификации NTLM гораздо сложнее процедуры LAN Manager.

NTLMv2

В итоге выяснилось, что и NTLM уязвим, и специалисты Microsoft подготовили NTLMv2, который до сих пор считается достаточно надежным, хотя сейчас предпочтительный протокол — Kerberos. NTLMv2 по-прежнему широко используется для локальной регистрации и в некоторых других случаях. NTLMv2 похож на NTLM, но в хеше пароля NTLMv2 используется аутентификация сообщений HMAC-MD5, а последовательности запрос—ответ присваивается метка времени, чтобы предотвратить атаки, в ходе которых взломщик записывает учетные данные и впоследствии их использует.

В целом NTLMv2 более устойчив к атакам с применением «грубой силы», нежели NTLM, так как в протоколе применяется 128-разрядный ключ шифрования. Известно только о двух программах взлома паролей (одна из них — LC5 компании Symantec), с помощью которых удавалось открыть хеши паролей NTLMv2.

Kerberos

Компания Microsoft приняла Kerberos в качестве выбираемого по умолчанию протокола доменной аутентификации для доменов Windows 2000, а затем и ActiveDirectory. Kerberos — открытый стандарт, пригодный для взаимодействия с инородными доменами (называемыми областями — realm — в UNIX и Linux). Каждый DomainController в доменах AD играет роль сервера распределения (Kerberos Distribution Server, KDC) и может участвовать в процедуре аутентификации. Безопасность повышается благодаря следующим характеристикам Kerberos:

- · взаимная аутентификация между клиентом и сервером;

· надежная защита пароля, так как Windows пересылает пароль только при начальном обращении, а не в каждом событии аутентификации и все сеансы связи шифруются;

· последовательность запрос-ответ с меткой времени не позволяет взломщику использовать перехваченный пароль по прошествии определенного времени;

· серверный процесс может обращаться к удаленному ресурсу от имени пользователя;

· интероперабельность – способность системы к взаимодействию с другими системами

Краткое описание работы Kerberos:

1После успешной обычной аутентификации компьютер пользователя запрашивает билет безопасности из сервера Kerberos (DC) для будущих запросов аутентификации.

2Сервер Kerberos выдает запросчику билет для участия в будущих событиях аутентификации и авторизации без повторного предъявления первоначальных учетных данных аутентификации.

3Когда запросчику нужно обратиться к ресурсу сервера-участника, он получает другой билет доступа от сервера Kerberos и предъявляет его серверу ресурса для проверки.

4Первоначальные учетные данные аутентификации не передаются по сетевым каналам ни в одном из последующих сеансов аутентификации (до тех пор, пока не истечет срок действия билета, выданного на этапе 2).

Следует обратить внимание, что, хотя принцип работы Kerberos напоминает инфраструктуру с частным открытым ключом (public key infrastructure, PKI), вся информация защищается с использованием симметричных ключей (в отличие от асимметричных ключей, применяемых в большинстве служб аутентификации).

Протоколы аутентификации для удалённого доступа

Часть протоколов сетевой аутентификации были разработаны специально для обеспечения удаленного доступа к информационным ресурсам посредством открытых каналов связи (к примеру, телефонные линии, Internet). В качестве примера можно привести протоколы PAP, CHAP, EAP, RADIUS, TACACS и другие. В качестве примера кратко рассмотрим работу протокола RADIUS.

Протокол аутентификации RADIUS

Протокол аутентификации Remote Authentication Dial-in User Service (RADIUS)2 рассматривается как механизм аутентификации и авторизации удалённых пользователей в условиях распределённой сетевой инфраструктуры, предоставляющий централизованные услуги по проверке подлинности и учёту для служб удалённого доступа.

В рамках стандарта выделяются следующие роли:

· Клиент RADIUS. Клиент RADIUS принимает от пользователей запросы на аутентификацию. Все принятые запросы переадресовываются серверу RADIUS для последующей аутентификации и авторизации. Как правило, в качестве клиента протокола RADIUS выступает сервер удалённого доступа.

· Сервер RADIUS. Основная задача сервера RADIUS заключается в централизованной обработке информации, предоставленной клиентами RADIUS. Один сервер способен обслуживать несколько клиентов RADIUS. Сервер осуществляет проверку подлинности пользователя и его полномочий. При этом в зависимости от реализации сервера RADIUS для проверки подлинности используются различные базы данных учётных записей.

· Посредник RADIUS. Взаимодействие клиентов и серверов RADIUS осуществляется посредством специальных сообщений. В распределённых сетях клиент и сервер RADIUS могут быть разделены различными сетевыми устройствами (такими, например, как маршрутизатор). Под посредником RADIUS понимается сетевое устройство, способное осуществлять перенаправление сообщений протокола RADIUS.

Поддержка протокола RADIUS реализована на многих современных платформах, что позволяет использовать его в межплатформенных решениях. В качестве примера сервера и посредника RADIUS можно привести реализованную в Windows Server 2003 службу проверки подлинности в Интернете (Internet Authentication Service, IAS). Эта служба позиционируется как механизм централизованной аутентификации и авторизации пользователей, использующих различные способы подключений к сети. Служба IAS интегрирована с другими сетевыми службами Windows Server

2003, такими, как служба маршрутизации и удалённого доступа и служба каталога Active Directory.

TACACS

TACACS (terminal access controller access control system) - собственно

система управления авторизацией и аутентификацией

TACACS - это протокол аутентификации маршрутизаторов Cisco

В данной статье я опишу основные принципы настройки сервера и клиента TACACS+(плюс указывает на версию протокола, которая используется в настоящее время).

TACACS имеет очень широкое применение, т.к. может обеспечивать работу всех

Ciscok с единым сервером авторизации, который также позволяет устанавливать привилегии различных пользователей в широких пределах, например, давать определённым пользователям доступ только к определённым командам, давать пользователям пользоваться определёнными сервисами только с заданных адресов, организовывать группы пользователей, вести лог-файл доступа пользователей (это особенно важно для маршрутизаторов, т.к. позволяет определить, какие пользователи и сколько пользовались определёнными сетевыми службами: ppp, slip и.т.д.), выполнять для пользователей определённые команды ОС.

Аутентификация на основе одноразовых паролей

Для организации удаленного доступа пользователей к защищенным информационным ресурсам были разработаны достаточно надежные схемы с применением одноразовых паролей (OTP – One Time Password). Суть концепции одноразовых паролей состоит в использовании различных паролей при каждом новом запросе на предоставление доступа. Одноразовый пароль действителен только для одного входа в систему. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от внешних угроз. Известно четыре метода аутентификации с применением технологии OTP:

- использование механизма временных меток на основе системы единого времени;
- применение общего пароля для легального пользователя и проверяющего списка случайных паролей и надежного механизма их синхронизации;
- использование общего пароля для пользователя и проверяющего генератора псевдослучайных чисел с одним и тем же начальным значением;
- применение фиксированного числа случайных (псевдослучайных) последовательностей, скопированных на носители в виде скретч-карт.

Наиболее распространены аппаратные реализации одноразовых паролей. Их называют OTP-токенами. Они имеют небольшой размер и выпускаются в виде различных форм-факторах:

- карманного калькулятора;
- брелока;
- смарт-карты;
- устройства, комбинированного с USB-ключом.

В качестве примера решений OTP можно привести линейку RSA SecurID, ActiveCard Token, комбинированный USB-ключ Aladdin eToken NG-OTP. В частности, одной из распространенных аппаратных реализаций одноразовых паролей является технология SecurID, предлагаемая компанией RSA Security. Она основана на специальных калькуляторах — токенах, которые каждую минуту генерируют новый код. В токен встроена батарейка, заряда которой хватает на 3 – 5 лет, после чего токен нужно менять. Аутентификация с помощью SecureID интегрирована в сотни приложений, а недавно при поддержке Microsoft она была встроена в операционную систему Windows. Впрочем, имеются реализации "в железе" и другие алгоритмы генерации одноразовых паролей. Например, можно генерировать пароль по событию — нажатию клавиши на устройстве. Такое решение предлагает компания Secure Computing в виде продукта Safeword. Аппаратную реализацию технологии "запрос-ответ" продает корпорация CryptoCard. Имеются даже универсальные аппаратные реализации, которые позволяют перепрограммировать токены. В частности, решения, выпускаемые компанией VASCO, допускают реализацию нескольких десятков алгоритмов аутентификации с помощью одноразовых паролей. В целом технология OTP основана на исполь-

зовании двухфакторных схем аутентификации и может быть классифицирована как усиленная технология аутентификации.

Аутентификация по предъявлению цифрового сертификата

Механизмы аутентификации с применением сертификатов обычно используют протокол с запросом и ответом. Согласно этому протоколу, сервер аутентификации направляет пользователю последовательность символов, называемую запросом, а программное обеспечение клиентского компьютера для генерирования ответа вырабатывает с помощью закрытого ключа пользователя цифровую подпись под запросом от сервера аутентификации. Общий процесс подтверждения подлинности пользователя состоит из следующих стадий:

- получение открытого ключа CA (одноразовый процесс),
- получение по некоторому незащищенному каналу от этого пользователя его сертификата открытого ключа.

Аутентификация с открытым ключом используется как защищенный механизм аутентификации в таких протоколах как SSL, а также может использоваться как один из методов аутентификации в рамках рассмотренных протоколов Kerberos и RADIUS.

SSL (Secure Sockets Layer — протокол защищённых сокетов) - криптографический протокол, призванный обеспечить безопасную передачу данных

по сети Интернет. При работе по этому протоколу создаётся защищённое соединение

между клиентом и сервером. По стандарту протокол работает на 443-м порту. SSL изначально разработан компанией Netscape Communications. Поддерживается всеми популярными браузерами.

Использование смарт-карт и USB-ключей

Несмотря на то, что криптография с открытым ключом согласно спецификации X.509 может обеспечивать строгую аутентификацию пользователя, сам по себе незащищенный закрытый ключ подобен паспорту без фотографии. Закрытый ключ, хранящийся на жёстком диске компьютера владельца, уязвим по отношению к прямым и сетевым атакам. Достаточно подготовленный злоумышленник может похитить персональный ключ пользователя и с помощью этого ключа представляться этим пользователем. Защита ключа с помощью пароля помогает, но недостаточно эффективно - пароли уязвимы по отношению ко многим атакам. Несомненно, требуется более безопасное хранилище.

Смарт-карты

Смарт-карты - пластиковые карты стандартного размера банковской карты, имеющие встроенную микросхему. Они находят всё более широкое применение в различных областях, от систем накопительных скидок до кредитных и дебетовых карт, студенческих билетов и телефонов стандарта GSM.

Для использования смарт-карт в компьютерных системах необходимо устройство чтения смарт-карт. Несмотря на название - устройство чтения (или считыватель), - большинство подобных оконечных устройств, или устройств сопряжения (IFD- InterFace Device), способны как считывать, так и записывать информацию, если позволяют возможности смарт-карты и права доступа. Устройства чтения смарт-карт могут подключаться к компьютеру посредством последовательного порта, слота PCMCIA или USB. Устройство чтения смарт-карт также может быть встроено в клавиатуру. Как правило, для доступа к защищенной информации, хранящейся в памяти смарт-карты, требуется пароль, называемый PIN-кодом.

USB-ключи

USB-ключи достаточно привлекательны, поскольку USB стал стандартным портом для подключения периферийных устройств и организации не нужно приобретать для пользователей какие бы то ни было считыватели.

Аутентификацию на основе смарт-карт и USB-ключей сложнее всего обойти, так как используется уникальный физический объект, которым должен обладать человек, чтобы войти в систему. В отличие от паролей, владелец быстро узнаёт о краже и может сразу принять необходимые меры для предотвращения её негативных последствий. Кроме того, реализуется двухфакторная аутентификация. Микропроцессорные смарт-карты и USB-ключи могут повысить надёжность

служб PKI- Public Key Infrastructure: смарт-карта может использоваться для безопасного хранения закрытых ключей пользователя, а также для безопасного выполнения криптографических преобразований. Безусловно, данные устройства аутентификации не обеспечивают абсолютную безопасность, но надёжность их защиты намного превосходит возможности обычного настольного компьютера.

Для хранения и использования закрытого ключа разработчики используют различные подходы. Наиболее простой из них - использование устройства аутентификации в качестве защищенного носителя аутентификационной информации: при необходимости карта экспортирует закрытый ключ, и криптографические операции осуществляются на рабочей станции. Этот подход является не самым совершенным с точки зрения безопасности, зато относительно легко реализуемым и предъявляющим невысокие требования к устройству аутентификации. Два других подхода более безопасны, поскольку предполагают выполнение устройством аутентификации криптографические операций. При первом пользователь генерирует ключи на рабочей станции и сохраняет их в памяти устройства. При втором пользователь генерирует ключи при помощи устройства. В обоих случаях, после того как закрытый ключ сохранён, его нельзя извлечь из устройства и получить любым другим способом.

Генерация ключевой пары вне устройства

В этом случае пользователь может сделать резервную копию закрытого ключа. Если устройство выйдет из строя, будет потеряно, повреждено или уничтожено, пользователь сможет сохранить тот же закрытый ключ в памяти нового устройства. Это необходимо, если пользователю требуется расшифровать какие-либо данные, сообщения, и т.д., зашифрованные с помощью соответствующего открытого ключа. Однако при этом закрытый ключ пользователя подвергается риску быть похищенным, что означает его компрометацию.

Генерация ключевой пары с помощью устройства

В этом случае закрытый ключ не появляется в открытом виде, и нет риска, что злоумышленник украдёт его резервную копию. Единственный способ использования закрытого ключа - это обладание устройством аутентификации. Являясь наиболее безопасным, это решение выдвигает высокие требования к возможностям самого устройства: оно должно обладать функциональностью генерации ключей и осуществления криптографических преобразований. Это решение также предполагает, что закрытый ключ не может быть восстановлен в случае выхода устройства из строя, и т. п. Об этом необходимо беспокоиться при использовании закрытого ключа для шифрования, но не там, где он используется для аутентификации или в других службах, использующих цифровые подписи.

Классификация методов идентификации и аутентификации с точки зрения применяемых технологий представлена на рис. 2.

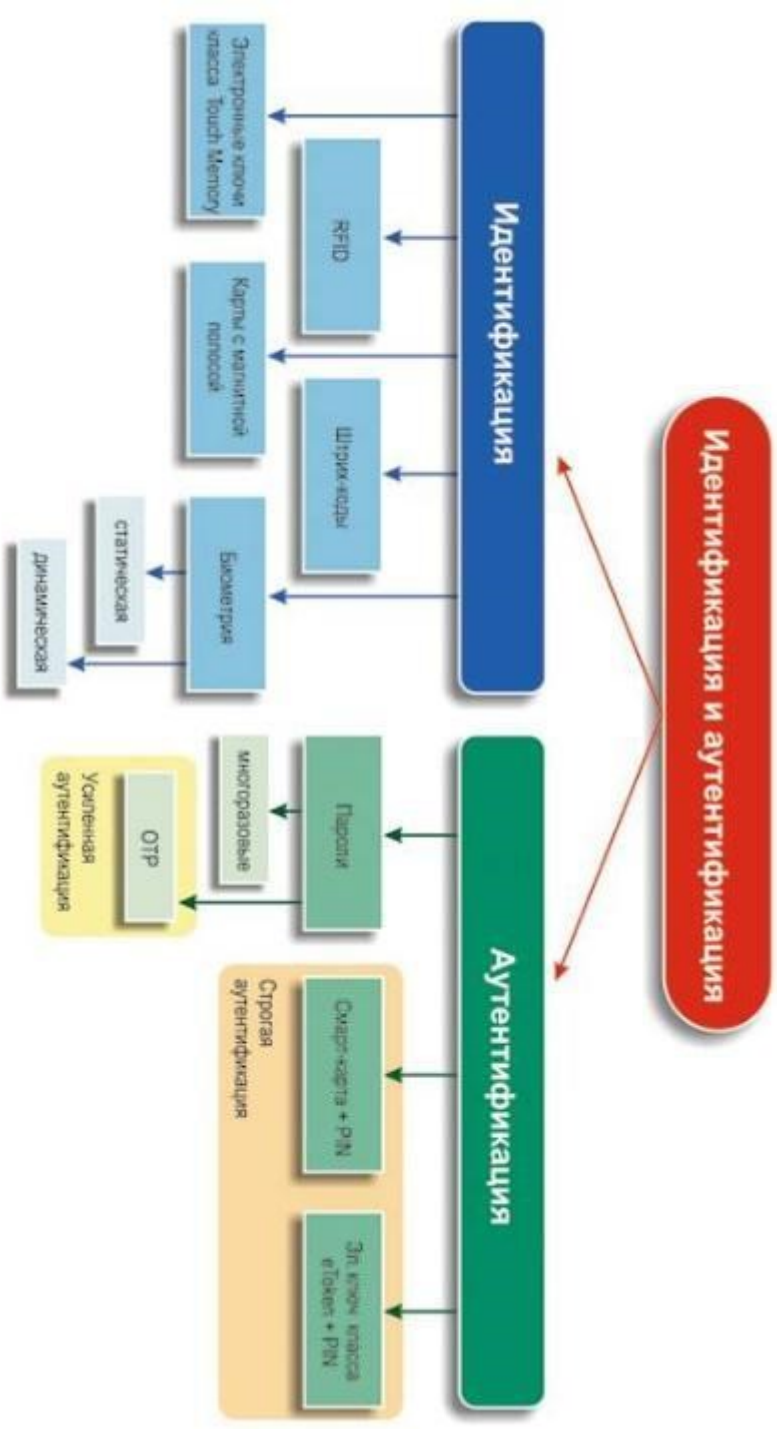



Рис.2. Классификация технологий идентификации и аутентификации

Основы межсетевого обмена в сетях TCP/IP

Структура стека протоколов TCP/IP

При рассмотрении процедур межсетевого взаимодействия всегда опираются на стандарты, разработанные International Standard Organization (ISO). Эти стандарты получили название "Семиуровневой модели сетевого обмена" или в английском варианте "Open System Interconnection Reference Model" (OSI Ref.Model). В данной модели обмен информацией может быть представлен в виде стека, представленного на рисунке 2.1. Как видно из рисунка, в этой модели определяется все - от стандарта физического соединения сетей до протоколов обмена прикладного программного обеспечения.

Рис. 2.1 Семиуровневая модель протоколов межсетевого обмена OSI

Физический уровень данной модели определяет характеристики физической сети передачи данных, которая используется для межсетевого обмена. Это такие параметры, как: напряжение в сети, сила тока, число контактов на разъемах и т.п. Типичными стандартами этого уровня являются, например RS232C, V35, IEEE 802.3 и т.п.

К канальному уровню отнесены протоколы, определяющие соединение, например, SLIP (Strial Line Internet Protocol), PPP (Point to Point Protocol), NDIS, пакетный протокол, ODI и т.п. Речь идет о протоколе взаимодействия между драйверами устройств и устройствами, с одной стороны, а с другой стороны, между операционной системой и драйверами устройства. Такое определение основывается на том, что драйвер - это, фактически, конвертор данных из оного формата в другой, но при этом он может иметь и свой внутренний формат данных.

К сетевому (межсетевому) уровню относятся протоколы, которые отвечают за отправку и получение данных, или, другими словами, за соединение отправителя и получателя. К этому уровню в TCP/IP относят протокол IP (Internet Protocol). Именно здесь определяется отправитель и получатель, именно здесь находится необходимая информация для доставки пакета по сети.

Транспортный уровень отвечает за надежность доставки данных, и здесь, проверяя контрольные суммы, принимается решение о сборке сообщения в одно целое. В Internet транспортный уровень представлен двумя протоколами TCP (Transport Control Protocol) и UDP (User Datagramm Protocol). Если предыдущий уровень (сетевой) определяет только правила доставки информации, то транспортный уровень отвечает за целостность доставляемых данных.

Уровень сессии определяет стандарты взаимодействия между собой прикладного программного обеспечения. Это может быть некоторый промежуточный стандарт данных или правила обработки информации. Условно к этому уровню можно отнеси механизм портов протоколов TCP и UDP и Berkeley Sockets.

Уровень обмена данными с прикладными программами (Presentation Layer) необходим для преобразования данных из промежуточного формата сессии в формат данных приложения. В Internet это преобразование возложено на прикладные программы.

Уровень прикладных программ или приложений определяет протоколы обмена данными этих прикладных программ. В Internet к этому уровню могут быть отнесены такие протоколы, как: FTP, TELNET, HTTP, GOPHER и т.п.

Вообще говоря, стек протоколов TCP отличается от только что рассмотренного стека модели OSI. Обычно его можно представить в виде схемы, представленной на рисунке 2.2.

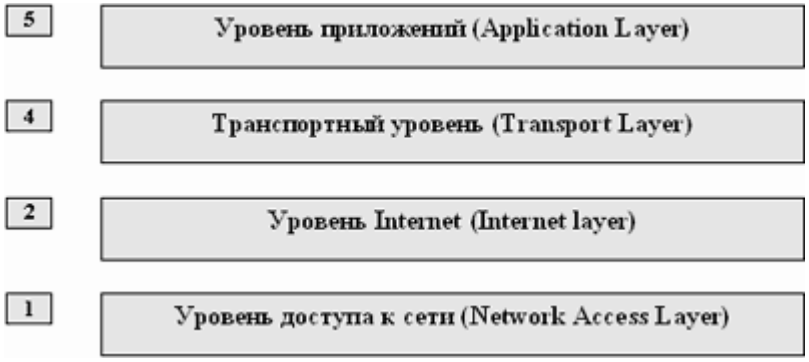


Рис. 2.2. Структура стека протоколов TCP/IP

В этой схеме на уровне доступа к сети располагаются все протоколы доступа к физическим устройствам. Выше располагаются протоколы межсетевого обмена IP, ARP, ICMP. Еще выше основные транспортные протоколы TCP и UDP, которые кроме сбора пакетов в сообщения еще и определяют какому приложению необходимо данные отправить или от какого приложения необходимо данные принять. Над транспортным уровнем располагаются протоколы прикладного уровня, которые используются приложениями для обмена данными.

Драйвер - программа, непосредственно взаимодействующая с сетевым адаптером.

Сетевой интерфейс - физическое устройство, подключающее компьютер к сети. В нашем случае - карта Ethernet.

Кадр - это блок данных, который принимает/отправляет сетевой интерфейс.

IP-пакет - это блок данных, которым обменивается модуль IP с сетевым интерфейсом.

UDP-датаграмма - блок данных, которым обменивается модуль IP с модулем UDP.

TCP-сегмент - блок данных, которым обменивается модуль IP с модулем TCP.

Прикладное сообщение - блок данных, которым обмениваются программы сетевых приложений с протоколами транспортного уровня.

Информационные сервисы Internet

Система Доменных Имен

Числовая адресация удобна для машинной обработки таблиц маршрутов, но совершенно не приемлема для использования ее человеком. Запомнить наборы цифр гораздо труднее, чем мнемонические осмысленные имена. Для облегчения взаимодействия в Сети сначала стали использовать таблицы соответствия числовых адресов именам машин. Эти таблицы сохранились до сих пор и используются многими прикладными программами. Некоторое время даже существовало центральное хранилище соответствий, которое можно было по FTP скачать на свою машину.

Если речь идет о системе типа Unix, то этот файл (hosts) расположен в директории /etc и имеет следующий вид:

| IP-адрес | имя машины | Синонимы(alias) |
|---|---|---|
| 127.0.0.1 | localhost | localhost |
| 144.206.160.32 | Polyn | polyn |
| 144.206.160.40 | Apollo | www |

Рис. 1 Пример таблицы имен хостов (файл /etc/hosts)

Файл hosts — текстовый файл, содержащий базу данных доменных имен и используемый при их трансляции в сетевые адреса узлов. Запрос к этому файлу имеет приоритет перед обращением к DNS-серверам. В отличие от DNS, содержимое файла контролируется администратором

компьютера. С помощью файла hosts возможно осуществлять фильтрацию рекламы, путём перенаправления доменных адресов баннеров на адрес 127.0.0.1.

Пользователь для обращения к машине может использовать как IP-адрес машины, так и ее имя или синоним (alias). синонимов может быть много, и, кроме того для разных IP-адресов может быть указано одно и то же имя.

В локальных сетях файлы hosts используются достаточно успешно до сих пор. Практически все операционные системы от различных клонов Unix до Windows NT поддерживают эту систему соответствия IP-адресов доменным именам.

Однако такой способ присвоения символьных имен был хорош до тех пор, пока Internet был маленьким. По мере роста сети стало затруднительным держать большие списки имен на каждом компьютере. Для того, что бы решить эту проблему, были придуманы DNS (Domain Name System).

На сегодняшний день большое количество вредоносных программ используют файл hosts для блокирования доступа к веб-сайтам популярных порталов или социальных сетей. Зачастую вместо блокировки сайтов вредоносные программы перенаправляют пользователя на страницы, внешне похожие на популярные ресурсы (социальные сети, почтовые сервисы и т.д.), куда невнимательный пользователь вводит учетные данные, попадающие таким образом к злоумышленникам. Также, возможно блокирование доступа к веб-сайтам компаний-разработчиков антивирусного программного обеспечения.

Следует отметить, что антивирусные программы, использующие проактивные методы защиты, как правило, запрещают изменение файла hosts неизвестному программному обеспечению.

### Принципы организации DNS

Любая DNS является прикладным процессом, который работает над стеком TCP/IP. Таким образом, базовым элементом адресации является IP-адрес, а доменная адресация выполняет роль сервиса.

DNS сервис - это информационный сервис Internet, и, следовательно, протоколы его реализующие относятся к протоколам прикладного уровня согласно стандартной модели OSI. Однако с точки зрения операционной системы поддержка DNS может входить в нее как компонента ядра, которая прикладным пользовательским процессом не является. Пользовательские программы общаются с ней при помощи системных вызовов. Такое положение вещей справедливо практически для всех Unix-систем. Другое дело системы на базе MS-DOS и Windows 3.x. В этих системах DNS (точнее ее клиентская часть) реализована как прикладная программа.

Система доменных адресов строится по иерархическому принципу. Однако иерархия эта не строгая. Фактически, нет единого корня всех доменов Internet. Если быть более точным, то такой корень в модели DNS есть. Он так и называется "ROOT". Однако, единого администрирования этого корня нет. Администрирование начинается с доменов верхнего, или первого, уровня. В 80-е годы были определены первые домены этого уровня: gov, mil, edu, com, net. Позднее, когда сеть перешагнула национальные границы США появились национальные домены типа: uk, jp, au, ch, и т.п. Для СССР также был выделен домен su. После 1991 года, когда республики союза стали суверенными, многие из них получили свои собственные домены: ua, ru, la, li, и т.п. Однако Internet не СССР, и просто так выбросить домен su из сервера имен нельзя, на основе доменных имен строятся адреса электронной почты и доступ ко многим другим информационным ресурсам Internet. Поэтому гораздо проще оказалось ввести новый домен к существующему, чем заменить его. Таким образом в Москве существуют организации с доменными именами, оканчивающимися на su (например, kiae.su) и оканчивающимися на ru (msk.ru).

Наиболее популярной программой поддержки DNS является named, которая реализует Berkeley Internet Name Domain (BIND). Но эта программа не единственная. Так в системе Windows NT 4.0 есть свой сервер доменных имен, который поддерживает спецификацию BIND. Определена в документе RFC 1033-1035.

### BIND (Berkeley Internet Name Domain)

BIND был создан студентами в начале 1980-х на грант, выданный DARPA и впервые был выпущен в BSD 4.3. Версия 9 была переписана заново компанией Nominum (англ.), релиз был вы-

пущен в сентябре 2000 года. Версия 10 содержит большое количество кода на Python. Ранние версии BIND хранили информацию только в текстовых файлах зон (англ.). Начиная с версии 9.4, в качестве хранилища можно использовать LDAP, Berkeley DB, PostgreSQL,MySQL и ODBC. В версиях до 9 было выявлено немало серьёзных проблем с безопасностью.

BIND или Berkeley Internet Name Domain - это сервер доменных имен реализованный в университете Беркли, который широко применяется на Intenet'e. Он обеспечивает поиск доменных имен и IP-адресов для любого узла Сети. BIND обеспечивает рассылку сообщений электронной почты через узлы Internet. Если говорить более точно BIND обеспечивает поиск доменного адреса машины пользователя, которому адресована почта, и определение IP-адреса доменному адресу. Эта информация используется программой рассылки почтовых сообщений sendmail, которая выступает в качестве почтового сервера. BIND реализован по схеме "клиент/сервер". Собственно BIND - это сервер, а функции клиента выполняет name resolver или просто resolver.

Регистрация доменных имен

Для того, чтобы получить зону надо отправить заявку в РосНИИРОС, который отвечает за делегирование поддоменов в пределах домена ru. В заявке указывается адрес компьютера-сервера доменных имен, почтовый адрес администратора сервера, адрес организации и ряд другой информации.

При заполнении этой заявки следует иметь в виду, что она будет обрабатываться роботом автоматом. Этот автомат проверяет ее на наличие ошибок заполнения и противоречия с существующей базой данных делегированных доменов. Так как робот не терпит неточностей и глух к различного рода просьбам, то заполнять заявку следует аккуратно. Автомат обрабатывает заявку, выделяет в ней записи для базы данных регистрации доменов. Сами эти записи состоят из полей. Каждое поле идентифицируется в заявке именем поля, после которого ставится символ ":".

```
domain: vega.ru
descr:  International Agency VEGA
descr:  Kurchatov sq. 1
descr:  115470 Moscow
descr:  Russian Federation
admin-c:        Pavel B Khramtsov
zone-c: Pavel B Khramtsov
tech-c: Pavel B Khramtsov
nserver:        vega-gw.vega.ru
nserver:        ns.relarn.ru
nserver:        polyn.net.kiae.su
dom-net:        194.226.43.0
changed:        paul@kiae.su 961018
source: RIPN
person: Pavel B Khramtsov
address:        International Agency Vega
address:        Kurchatov sq. 1
address:        115470 Moscow
address:        Russian Federation
phone:  +7 095 1969124
fax-no: +7 095 9393670
e-mail: paul@kiae.su
changed:        paul@kiae.su 961018
source: RIPN
```

В строке описания поля "domain:" указывается имя домена, которое вы просите зарегистрировать. РосНИИРОС регистрирует только поддомены домена ru.

В строке описания поля "descr:" указывают название и адрес организации, которая запрашивает домен. Так как на одной строке эта информация не может разместиться, то команд descr может быть несколько.

В строке описания поля "admin-c:" указывается персона, которая осуществляет администрирование домена. Поле имеет обязательный формат: <имя> <первая буква отчества> <фамилия>. Таких строк может быть несколько, если лиц отвечающих за администрирование домена больше одного. Вместо указанного выше формата можно использовать также и идентификатор персоны, если таковой имеется. Идентификатор называют nichandle, или персональный код. zone-c и tech-c . Обычно для наших доменов admin-c, zone-c и tech-c один и тот же человек. Поле "tech-c:" указывается для технического администратора домена, к которому обращаются в случае экстренных ситуаций. Формат этого поля совпадает с форматом команды admin-c. и «zone-c» . Мало кто может позволить роскошь держать сразу трех разных специалистов на обслуживании сервиса доменных имен. Учитывая отечественные реалии, можно со всей ответственностью утверждать, что кроме неразберихи ни к чему другому большое количество администраторов не приводит.

В строке описания поля "nserver:" указывают доменные имена серверов зоны. Как правило, таких строк в заявке бывает несколько. Первым указывается primary или главный сервер домена. На этом сервере хранится база данных домена. Вторым указывается secondary или дублирующий сервер домена. Дублирующие сервера призваны повысить надежность работы всей системы доменных имен, поэтому дублирующих серверов может быть несколько. Если существуют другие дублирующие сервера, то указываются и они. При указании дублирующих серверов первым следует указывать тот, который наиболее надежно обслуживает запросы к домену. Если хотя бы один из них не откликается на запросы автомата, то заявка отклоняется.

Поле "sub-dom:" описывает поддомены домена.

Поле "dom-net:" указывает на список IP-сетей данного домена. Если у организации, которая заводит свой собственный домен имеется в наличии несколько сетей, то эти сети можно указать в этом поле, разделяя их пробелами.

Поле "changed:" является обязательным и служит указателем на то лицо, которое последним вносило изменения в заявку. В качестве значения поля после символа ":" указывается почтовый адрес этого лица и, через пробел дата внесения изменения в формате ГГММДД (Г-год, М-месяц, Д-день).

Последняя запись в заявке - это поле source, которое отделяет различные записи во входном потоке данных программы робота. Значение этого поля - RIPN.

Вслед за записью заявки следует запись описания персоны. Именно эта запись позволяет связывать поля admin-c, zone-c, tech-c с информацией о конкретном лице, которая содержится в записи описания персоны.

Запись описания персоны начинается с поля "person:". В данном поле указывается информация о лице (персоне). Обычно, данное поле имеет следующий формат:

<имя> <первая буква отчества> <фамилия>.

Поле "address:" вслед за полем "person:". Данное поле состоит из нескольких строк, каждая из которых начинается с имени поля. Первым указывается организация, во второй строке - улица и номер дома, в третьей - почтовый индекс и название города или поселка, в последней строке - название страны. Одним словом - это типичный американский почтовый адрес.

За адресом следует поле "phone:". В нем указывается номер телефона, по которому можно связаться с указанным лицом. Номер задается с указанием номера страны и кода города. Для Москвы - +7 095 ___ __ __. Телефонов можно указать несколько.

Все выше сказанное для поля "phone:" относится и к полю "fax-no:". В этом поле указывается номер телефакса.

"e-mail:", хотя оно и не является обязательным полем заявки.

В поле "nic-hdl:" указывается персональный номер пользователя, если он у данного пользователя есть. Поле не является обязательным, но, как подчеркивается в инструкции по заполнению заявок "крайне желательно".

Последним полем в описании персоны, является поле "source:". В заявке можно указать несколько персон, что породит для каждой из них свою собственную запись в базе данных описания доменов. Информация о зоне и лицах, которые ответственны за ведение зоны (и не только о них) можно найти используя сервис whois ,например, на

whois.ripn.net <имя зоны или персоны>

% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

domain: URFU.RU
nserver: ns1.urfu.ru. 212.193.66.21
nserver: ns2.urfu.ru. 212.193.82.21
nserver: ns3.urfu.ru. 212.193.72.21
state: REGISTERED, DELEGATED, VERIFIED
org: federalnoe gosudarstvennoe avtonomnoe obrazovatelnoe uchrezhdenie visshego professionalnogo obrazovaniya "UrFU imeni pervogo Prezidenta Rossii B.N.Elcina"
registrar: REGRU-REG-RIPN
admin-contact: http://www.reg.ru/whois/admin_contact
created: 2008.12.16
paid-till: 2013.12.16
free-date: 2014.01.16
source: TCI

nic-hdl: REGRU-REG-RIPN
org: Domain Registrar REG.RU
phone: +7 495 5801111
fax-no: +7 495 4915553
e-mail: info@reg.ru
www: http://www.reg.ru/whois/admin_contact
whois: whois.reg.ru
source: TCI

Last updated on 2013.03.04 20:36:36 MSK

Теперь после описания самой заявки перейдем к описанию ее регистрации. После того как заявка отправлена, следует настроить и запустить сервер в локальном режиме. Администратор РосНИИРОС обычно извещает о том, что у администрации домена ru нет претензий к вашей заявке и разрешает запустить ваш сервер для тестирования. Если в домене есть уже запрашиваемый вами поддомен или у администрации домена ru есть другие возражения по поводу регистрации вашего домена, то администрация домена ru вас об этом известит.

Если у администратора домена ru нет причин для отказа в регистрации, то он разрешает запуск сервера для тестирования. Если ваш сервер уже запущен, то это сообщение вы просто примете к сведению, если нет, то нужно срочно, обычно в течении 2-х часов настроить и запустить сервер (вообще-то, запускать надо сразу как только решили отправлять заявку).

Так, например, регистрация домена vega.ru длилась почти два месяца из-за того, что в начале были ошибки в заявке, потом были выявлены несоответствия заявки и описания зоны, затем сломался автомат регистрации и заявка была утеряна. Затем возникли проблемы с дублирующим сервером зоны (слишком большое время отклика, из-за которого автомат отклонял заявку).

При размещении сервера домена следует позаботиться о том, чтобы существовал вторичный (secondary) сервер имен вашего домена. Согласно большинству рекомендаций, следует иметь от 2-х до 4-х серверов на случай отказа основного сервера доменных имен.

Вообще говоря, можно вести переговоры о создании вторичного сервера доменных имен и с самим РосНИИРОС и с любым провайдером. Но за услуги последнего придется заплатить. Можно запустить вторичный сервер и на одном из своих компьютеров, но в этом случае вы просто выполните требования РосНИИРОС формально, так как надежности процедуре разрешения имен вашего домена такое решение не принесет.

Если система не может разрешить доменное имя, то она сообщает - "unknown host", т.е. система такого компьютера не знает. Если же доменное имя успешно транслируется в IP-адрес, то, в случае потери связи, система сообщает - "host un-reachable", т.е. система знает о такой машине, но в данный момент достичь эту машину нет никакой возможности.

В РосНИИРОС регистрируют не только "прямую" зону, но также и "обратную". Это две самостоятельные заявки. Понятие "прямая" зона - с английского - forward zone, а понятие "обратная" зона - reverse zone. "Прямая" зона определяет соответствие доменного имени IP-адресу, в то время, как "обратная" зона определяет обратное соответствие IP-адреса доменному имени.

Серверы доменных имен

Речь пойдет о программе, которая называется named. Именно она используется в большинстве Unix-систем в качестве реализации Berkeley Internet Name Domain - BIND.

Как и любой другой сервис прикладного уровня, а система доменных имен - это сервис прикладного уровня, программа named использует транспорт TCP и UDP (порты 53). Сервис BIND строится по схеме "клиент-сервер". В качестве клиентской части выступает процедура разрешения имен - resolver, а в качестве сервера, в нашем случае, программа named.

Resolver, собственно, не является какой-либо программой. Это набор процедур из системной библиотеки, которые позволяют прикладной программе, отредактированной с ними, получать по доменному имени IP-адрес компьютера или по IP-адресу доменное имя. Сами эти процедуры обращаются к системной компоненте resolver, которая ведет диалог с сервером доменных имен и таким образом обслуживает запросы прикладных программ пользователя.

На запросы описанных выше функций в системах Unix отвечает программа named. Идея этой программы проста - обеспечить как разрешение, так называемых, "прямых" запросов, когда по имени ищут адрес, так и "обратных", когда по адресу ищут имя. Управляется named специальной базой данных, которая состоит из нескольких фалов, и содержит соответствия между адресами и именами, а также адреса других серверов BIND, к которым данный сервер может обращаться в процессе поиска имени или адреса.

DNS и безопасность

В сентябре 1996 года многие компьютерные издания Москвы опубликовали материал, в котором рассматривался случай подмены доменных адресов World Wide Web сервера агенства InfoART, что привело к тому, что подписчики этого сервиса в течении некоторого времени вместо страниц этого агенста просматривали картинки "для взрослых".

Администрирование DNS осуществляла компания Demos, поэтому пресс-конференцию по поводу этого случая Demos и InfoArt проводили совместно. Разъяснения провайдера главным образом свелись к тому, что в базе данных DNS самого Demos никаких изменений не проводилось, а за состояние баз данных secondary серверов Demos ответственности не несет. Почему такое заявление вполне оправдывает провайдера?

Как было указано раньше, обслуживание запросов на получение IP-адресов по доменным именам, а именно об этом идет речь в случае InfoArt, осуществляется не одним сервером доменных имен, а множеством серверов. Все secondary серверы копируют базу данных с primary сервера, но делают они это с достаточно большими интервалами, иногда не чаще одного раза в двое суток.

Запрос разрешает тот сервер, который быстрее откликается на запрос клиента. Таким образом, если подправить информацию на secondary сервере о базе данных primary сервера, то можно действительно на время между копированиями описания зоны заставить пользователей смотреть

совсем не то, что нужно. Таким образом, практически все провайдеры попадают в категорию неблагонадежных. Но провайдеры также могут оказаться не при чем.

В принципе, любой администратор может запустить у себя на машине DNS и скопировать зону с primary сервера, не регистрируя ее в центре управления сетью. Это обычная практика, т.к. разрешение имен - главный тормоз при доступе к удаленной машине, и часто по timeout прерывается работа с ресурсом из-за невозможности быстрого разрешения имени. Таким образом, все администраторы сети попадают в потенциальных злоумышленников. Но на самом деле существуют еще и другие способы.

Существует несколько способов ограничения этого произвола. Первый из них - это точное знание IP-адресов ресурсов. В этом случае можно проверить состояние ресурса и выявить причину ошибки. Второй сопособ, запретить копировать описание зоны кому не поподя. Современные программы DNS позволяют описывать IP-адреса сетей, из которых можно копировать зоны. Правда такая политика должна быть согласована с другими владельцами зоны, в противном случае зону скопируют с secondary сервера. И наиболее мягкое средство - уменьшение времени хранения записей в кэше.

Для защиты можно использовать и фильтрацию пакетов. Зоны раздаются только по 53 порту TCP, в отличии от простых запросов. Если определить правила работы по этому порту, используя межсетевой фильтр, то можно и ограничить произвол при копировании информации с сервера доменных имен. Вообще, не стоит относиться к серверу доменных имен легкомысленно. Следует учитывать тот факт, что используя этот сервис, можно выявить структуру вашей локальной сети.

Информационные сервисы Internet2

4.1 Электронная почта в Internet

Электронная почта - один из важнейших информационных ресурсов Internet. Она является самым массовым средством электронных коммуникаций. Любой из пользователей Internet имеет свой почтовый ящик в сети.

4.1.1. Принципы организации

Электронная почта во многом похожа на обычную почтовую службу. Корреспонденция, подготавливается пользователем на своем рабочем месте либо программой подготовки почты, либо просто обычным текстовым редактором. Обычно, программа подготовки почты вызывает текстовый редактор, который пользователь предпочитает всем остальным программам этого типа. Затем пользователь должен вызвать программу отправки почты (программа подготовки почты вызывает программу отправки автоматически).

Для работы электронной почты в Internet разработан специальный протокол Simple Mail Transfer Protocol (SMTP), который является протоколом прикладного уровня и использует транспортный протокол TCP. Однако, совместно с этим протоколом используется и Unix-Unix-CoPy (UUCP) протокол. UUCP хорошо подходит для использования телефонных линий связи. Разница между SMTP и UUCP заключается в том, что при использовании первого протокола почтовый сервис пытается найти машину-получателя почты и установить с ней взаимодействие в режиме on-line для того, чтобы передать почту в ее почтовый ящик. В случае использования SMTP почта достигает почтового ящика получателя за считанные минуты и время получения сообщения зависит только от того, как часто получатель просматривает свой почтовый ящик. При использовании UUCP почта передается по принципу "stop-go", т.е. почтовое сообщение передается по цепочке почтовых серверов от одной машины к другой пока не достигнет машины-получателя или не будет отвергнуто по причине отсутствия абонента-получателя. С одной стороны, UUCP позволяет доставлять почту по плохим телефонным каналам, т.к. не требуется поддерживать линию в течении времени доставки от отправителя к получателю, а с другой стороны бывает обидно получить возврат сообщения через сутки после его отправки из-за того, что допущена ошибка в имени пользователя. В целом же общие рекомендации таковы: если имеется возможность надежно работать в режиме on-line и это является нормой, то следует настраивать почту для работы по протоколу SMTP, если линии связи плохие или on-line используется чрезвычайно редко, то лучше использовать UUCP.

Основой любой почтовой службы является система адресов. Без точного адреса невозможно доставить почту адресату. В Internet принята система адресов, которая базируется на доменном адресе машины, подключенной к сети.

4.1.2. Формат почтового сообщения (RFC-822)

Формат почтового сообщения Internet определен в документе RFC-822 (Standard for ARPA Internet Text Message). Это довольно большой документ объемом в 47 страниц машинописного текста. Почтовое сообщение состоит из трех частей: конверта, заголовка и тела сообщения. Пользователь видит только заголовок и тело сообщения. Конверт используется только программами доставки. Заголовок всегда находится перед телом сообщения и отделен от него пустой строкой. RFC-822 регламентирует содержание заголовка сообщения. Заголовок состоит из полей. Поля состоят из имени поля и содержания поля. Имя поля отделено от содержания символом ":". Минимально необходимыми являются поля Date, From, To.

Поле Date определяет дату отправки сообщения, поле From - отправителя, а поля To - получателя(ей). Чаще заголовок содержит дополнительные поля:

поле Sender указывает на отправителя. Поле Message-ID содержит уникальный идентификатор сообщения и используется программами доставки почты. Поле Subject определяет тему сообщения, Reply-To - пользователя, которому отвечают, Comment – комментарий. Поле Received: содержит транзитные адреса почтовых серверов с датой и временем прохождения сообщения. Вся эта информация полезна при разборе трудностей с доставкой почты.

Следует сказать, что формат сообщения постоянно дополняется и совершенствуется. В заключении хотелось бы отметить, что возможности почты не ограничиваются только пересылкой корреспонденции. По почте можно получить доступ ко многим ресурсам Internet, которые имеют почтовых роботов, отвечающих на запросы страждущих. Поэтому имеет смысл более детально изучить программное обеспечение, поддерживающее e-mail. Время, затраченное на чтение документации и опыты, окупятся возможностью получения информации из информационных архивов сети.

4.1.3. Формат представления почтовых сообщений MIME и его влияние на информационные технологии Internet

Стандарт MIME (Multipurpose Internet Mail Extensions или в нотации Internet, RFC-1341) предназначен для описания тела почтового сообщения Internet. Предшественником MIME является Стандарт почтового сообщения ARPA (RFC-822). Стандарт RFC-822 был разработан для обмена текстовыми сообщениями. С момента опубликования стандарта возможности аппаратных средств и телекоммуникаций ушли далеко вперед и стало ясно, что многие типы информации, которые широко используются в сети, невозможно передать по почте без специальных преобразований. Так в тело сообщения нельзя включить графику, аудио, видео и другие типы информации. RFC-822 не дает возможностей для передачи даже текстовой информации, которую нельзя реализовать 7-битовой кодировкой ASCII. Естественно, что при использовании RFC-822 не может быть и речи о передаче размеченного текста для отображения его различными стилями. Ограничения RFC-822 становятся еще более очевидными, когда речь заходит об обмене сообщениями в разных почтовых системах.

В некотором смысле стандарт MIME ортогонален стандарту RFC-822. Если последний подробно описывает в заголовке почтового сообщения текстовое тело письма и механизм его рассылки, то MIME, главным образом, ориентирован на описание в заголовке письма структуры тела почтового сообщения и возможности составления письма из информационных единиц различных типов.

В стандарте зарезервировано несколько способов представления разнородной информации. Для этого используются специальные поля заголовка почтового сообщения:

- поле версии MIME, которое используется для идентификации сообщения, подготовленного в новом стандарте;
- поле описания типа информации в теле сообщения, которое позволяет обеспечить правильную интерпретацию данных;

· поле типа кодировки информации в теле сообщения, указывающее на тип процедуры декодирования;

· два дополнительных поля, зарезервированных для более детального описания тела сообщения.

Стандарт MIME разработан как расширяемая спецификация, в которой подразумевается, что число типов данных будет расти по мере развития форм представления данных. При этом следует учитывать, что анархия типов (безграничное их увеличение) тоже не допустима.

4.1.4 Поля в MIME

Поле версии MIME (MIME-Version) Поле версии указывается в заголовке почтового сообщения и позволяет программе рассылки почты определить, что сообщение подготовлено в стандарте MIME. Поле версии указывается в общем заголовке почтового сообщения и относится ко всему сообщению целиком. Необходимо отметить, что в отличии от стандарта RFC-822 стандарт MIME позволяет перемешивать поля заголовка сообщения с телом сообщения. Поэтому все поля делятся на два класса: общие поля заголовка, которые записываются в начале почтового сообщения и частные поля заголовка, которые относятся только к отдельным частям составного сообщения и записываются перед ними.

Поле типа содержания тела почтового сообщения (Content-Type) Поле типа используется для описания типа данных, которые содержатся в теле почтового сообщения. Это поле сообщает программе чтения почты, какого сорта преобразования необходимы для того, чтобы сообщение правильно проинтерпретировать. Эта же информация используется и программой рассылки при кодировании/декодировании почты. Стандарт MIME определяет семь типов данных, которые можно передавать в теле письма:

текст (text); смешанный тип (multipart); почтовое сообщение (message); графический образ (image); аудио-информация (audio); фильм или видео (video); приложение (application).

Поле типа кодирования почтового сообщения (Content-Transfer-Encoding) Многие данные передаются по почте в их исходном виде. Это могут быть 7bit символы, 8bit символы, 64base символы и т.п. Однако, при работе в разнородных почтовых средах необходимо определить механизм их представления в стандартном виде.

Дополнительные необязательные поля "Content-ID" и "Content-Description". Первое поле определяет уникальный идентификатор содержания, а второе служит для комментария содержания. Ни то, ни другое программами просмотра, обычно, не отображаются.

4.1.5 Протокол обмена почтой SMTP (Simple Mail Transfer Protocol)

Протокол SMTP был разработан для обмена почтовыми сообщениями в сети Internet. SMTP не зависит от транспортной среды и может использоваться для доставки почты в сетях с протоколами, отличными от TCP/IP и X.25. Достигается это за счет концепции IPCE (Inter-Process Communication Environment). IPCE позволяет взаимодействовать процессам, поддерживающим SMTP, в интерактивном режиме, а не в режиме "STOP-GO".

Модель протокола. Взаимодействие в рамках SMTP строится по принципу двусторонней связи, которая устанавливается между отправителем и получателем почтового сообщения. При этом отправитель инициирует соединение и посылает запросы на обслуживание, а получатель - отвечает на эти запросы. Фактически, отправитель выступает в роли клиента, а получатель - сервера.

4.2 Эмуляция удаленного терминала. Удаленный доступ к ресурсам сети

Telnet - это одна из самых старых информационных технологий Internet. Она входит в число стандартов, которых насчитывается три десятка на полторы тысячи рекомендуемых официальных материалов сети, называемых RFC (Request For Comments).

Под telnet понимают триаду, состоящую из:

· telnet-интерфейса пользователя;

· telnetd-процесса;

· TELNET-протокола.

Эта триада обеспечивает описание и реализацию сетевого терминала для доступа к ресурсам удаленного компьютера.

4.2.1 Протокол Telnet

Telnet как протокол описан в RFC-854 (май, 1983 год). Его авторы J.Postel и J.Reynolds во введении к документу определили назначение telnet так: "Назначение TELNET-протокола - дать общее описание, насколько это только возможно, двунаправленного, восьмибитового взаимодействия, главной целью которого является обеспечение стандартного метода взаимодействия терминального устройства и терминал-ориентированного процесса. При этом этот протокол может быть использован и для организации взаимодействий "терминал-терминал" (связь) и "процесс-процесс" (распределенные вычисления)."

Telnet строится как протокол приложения над транспортным протоколом TCP. В основу telnet положены три фундаментальные идеи:

- концепция сетевого виртуального терминала (Network Virtual Terminal) или NVT;
- принцип договорных опций (согласование параметров взаимодействия);
- симметрия связи "терминал-процесс".

При установке telnet-соединения программа, работающая с реальным терминальным устройством, и процесс обслуживания этой программы используют для обмена информацией спецификацию представления правил функционирования терминального устройства или Сетевой Виртуальный Терминал (Network Virtual Terminal). Для краткости будем обозначать эту спецификацию NVT. NVT - это стандартное описание наиболее широко используемых возможностей реальных физических терминальных устройств. NVT позволяет описать и преобразовать в стандартную форму способы отображения и ввода информации. Терминальная программа ("user") и процесс ("server"), работающий с ней, преобразовывают характеристики физических устройств в спецификацию NVT, что позволяет, с одной стороны, унифицировать характеристики физических устройств, а с другой обеспечить принцип совместимости устройств с разными возможностями. Характеристики диалога диктуются устройством с меньшими возможностями. Если взаимодействие осуществляется по принципу "терминал-терминал" или "процесс-процесс", то "user" - это сторона, инициирующая соединение, а "server" - пассивная сторона.

Принцип договорных опций или команд позволяет согласовать возможности представления информации на терминальных устройствах. NVT - это минимально необходимый набор параметров, который позволяет работать по telnet даже самым допотопным устройствам, реальные современные устройства обладают гораздо большими возможностями представления информации. Принцип договорных команд позволяет использовать эти возможности. Например, NVT является терминалом, который не может использовать функции управления курсором, а реальный терминал, с которого осуществляется работа, умеет это делать. Используя команды договора, терминальная программа предлагает обслуживающему процессу использовать Esc-последовательности для управления выводом информации. Получив такую команду процесс начинает вставлять управляющие последовательности в данные, предназначенные для отображения.

Симметрия взаимодействия по протоколу telnet позволяет в течении одной сессии программе-"user" и программе-"server" меняться местами. Это принципиально отличает взаимодействие в рамках telnet от традиционной схемы "клиент-сервер". Симметрия взаимодействия тесно связана с процессом согласования формы обмена данными между участниками telnet-соединения. Когда речь идет о работе на удаленной машине в режиме терминала, то возможности ввода и отображения информации определяются только конкретным физическим терминалом и договорной процесс сводится к заказу терминальной программой характеристик этого терминала. Гораздо сложнее обстоит дело, когда речь идет об обмене информацией между двумя терминальными программами в режиме "терминал-терминал". В этом случае каждая из сторон может выступать инициатором изменения принципов представления информации и здесь проявляется еще одна особенность протокола telnet. Протокол не использует принцип "запрос-подтверждение", а применяет принцип "прямого действия". Это значит, что если терминальная программа хочет расширить возможности представления информации, то она делает это (например, вставляет в информационный поток Esc-

последовательности), если в ответ она получает информацию в новом представлении, то это означает, что попытка удалась, в противном случае происходит возврат к стандарту NVT.

Обычно процесс согласования форм представления информации происходит в начальный момент организации telnet-соединения. Каждый из процессов старается установить максимально возможные параметры сеанса. Однако эти параметры могут быть изменены и позже, в процессе взаимодействия (например, после запуска прикладной программы).

Сетевой виртуальный терминал (NVT). Концепция сетевого виртуального терминала позволяет обеспечить доступ к ресурсам удаленной машины с любого терминального устройства. Под терминальным устройством понимают любую комбинацию физических устройств, позволяющих вводить и отображать информацию. NVT предполагается буферизованным устройством. Это означает, что данные, вводимые с клавиатуры, не посылаются сразу по сети, а собираются в пакеты, которые отправляются либо по мере заполнения буфера, либо по специальной команде. Такая организация NVT призвана с одной стороны минимизировать сетевой трафик, а с другой обеспечить совместимость с реальными буферизованными терминалами.

4.3 Обмен файлами. Служба архивов FTP

FTP-архивы являются одним из основных информационных ресурсов Internet. Фактически, это распределенный депозитарий текстов, программ, фильмов, фотографий, аудио записей и прочей информации, хранящейся в виде файлов на различных компьютерах во всем мире.

4.3.1. Типы информационных ресурсов

Информация в FTP-архивах разделена на три категории:

· Защищенная информация, режим доступа к которой определяется ее владельцами и разрешается по специальному соглашению с потребителем. К этому виду ресурсов относятся коммерческие архивы (например, коммерческие версии программ в архивах ftp.microsoft.com или ftp.bsdi.com), закрытые национальные и международные некоммерческие, частная некоммерческая информация со специальными режимами доступа.

· Информационные ресурсы ограниченного использования, к которым относятся, например, программы класса shareware (Trumpet Winsock, Atis Mail, Netscape, и т.п.). В данный класс могут входить ресурсы ограниченного времени использования

· Свободно распространяемые информационные ресурсы или freeware, если речь идет о программном обеспечении. К этим ресурсам относится все, что можно свободно получить по сети без специальной регистрации. Это может быть документация, программы или что-либо еще.

Стержень технологии составляет FTP-протокол.

3.4.2. Протокол FTP

FTP (File Transfer Protocol или "Протокол Передачи Файлов") - один из старейших протоколов в Internet и входит в его стандарты. Обмен данными в FTP проходит по TCP-каналу. Построен обмен по технологии "клиент-сервер". В FTP соединение инициируется интерпретатором протокола пользователя. Управление обменом осуществляется по каналу управления в стандарте протокола TELNET. Команды FTP генерируются интерпретатором протокола пользователя и передаются на сервер. Ответы сервера отправляются пользователю также по каналу управления. В общем случае пользователь имеет возможность установить контакт с интерпретатором протокола сервера и отличными от интерпретатора пользователя средствами. Команды FTP определяют параметры канала передачи данных и самого процесса передачи. Они также определяют и характер работы с удаленной и локальной файловыми системами.

Сессия управления инициализирует канал передачи данных. При организации канала передачи данных последовательность действий другая, отличная от организации канала управления. В этом случае сервер инициирует обмен данными в соответствии с согласованными в сессии управления параметрами.

Режимы обмена данными

В протоколе большое внимание уделяется различным способам обмена данными между машинами различных архитектур. В общем случае, с точки зрения FTP, обмен может быть поточный или блоковый, с кодировкой в промежуточные форматы или без нее, текстовый или двоичный. При текстовом обмене все данные преобразуются в ASCII и в этом виде передаются по сети.

4.4 Информационно-поисковые системы Internet

Такие имена информационных служб как Lycos, AltaVista, Yahoo, OpenText, InfoSeek и ряд других, хорошо известны пользователям Internet. Без пользования услугами этих систем практически нельзя найти что-либо полезное в море информационных ресурсов Сети. Информационно-поисковые системы появились на свет достаточно давно. Теории и практике построения таких систем посвящено довольно большое количество статей, основная масса которых приходится на конец 70-х - начало 80-х годов.

4.4.1 Архитектура современных информационно-поисковых систем

Поэтому рассмотрим эту схему:

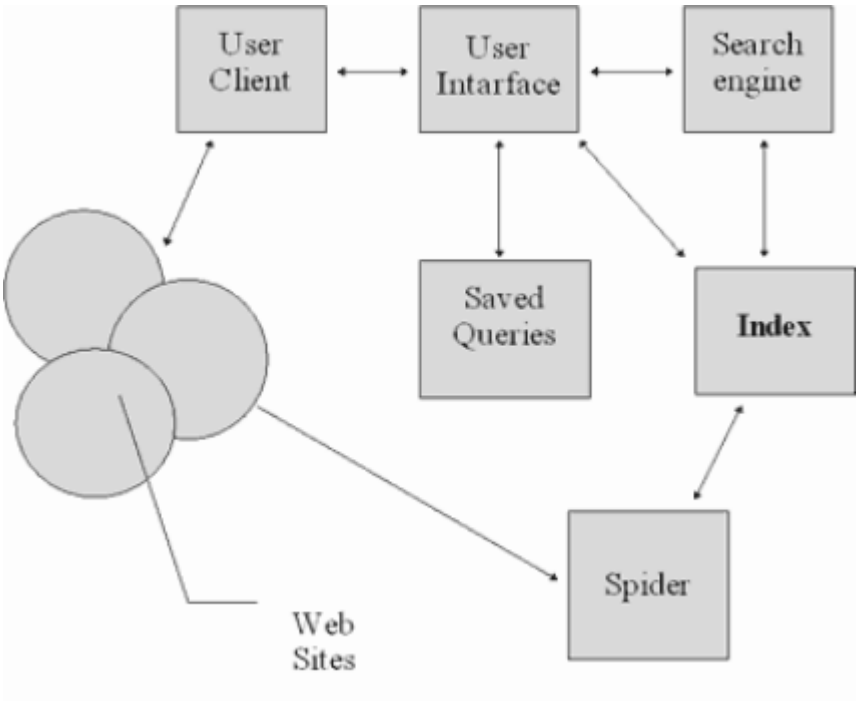



Рис. 3.41. Структура ИПС для Internet (Budi Yuwono, Dik L.Lee. Search and Ranking Algorims for Locating Resources on the World Wide Web)

client - это программа просмотра конкретного информационного ресурса. В настоящее время наиболее популярны мультипротокольные программы типа Netscape Navigator. Такая программа обеспечивает просмотр документов World Wide Web, FTP-архивов, почтовых списков рассылки и групп новостей Usenet. В свою очередь все эти информационные ресурсы являются объектом поиска информационно-поисковой системы.

user interface - интерфейс пользователя - это не просто программа просмотра. В случае информационно-поисковой системы под этим словосочетанием понимают и способ общения пользователя с поисковым аппаратом системы, т.е. с системой формирования запросов и просмотров результатов поиска.

earch engine - поисковая машина служит для трансляции запроса пользователя, который подготавливается на информационно-поисковом языке (ИПЯ), в формальный запрос системы, поиска ссылок на информационные ресурсы Сети и выдачи результатов этого поиска пользователю.

index database - индекс - это основной массив данных информационно-поисковой системы. Он служит для поиска адреса информационного ресурса. Архитектура индекса устроена таким образом, чтобы поиск происходил максимально быстро и при этом можно было бы оценить ценность каждого из найденных информационных ресурсов сети.

queries - запросы пользователя сохраняются в его личной базе данных. На отладку каждого запроса уходит достаточно много времени, и поэтому чрезвычайно важно хранить запросы, на которые система дает хорошие ответы.

index robot - робот-индексировщик служит для сканирования Internet и поддержки базы данных индекса в актуальном состоянии. Эта программа является основным источником информации о состоянии информационных ресурсов сети.

www sites - это весь Internet. А если говорить более точно, то это те информационные ресурсы, просмотр которых обеспечивается программами просмотра.

4.4.2 Информационные ресурсы и их представление в информационно-поисковой системе

Документальным массивом ИПС Internet является все множество документов основных типов: WWW-страницы, Gopher-файлы, документы Wais, записи архивов FTP, новости Usenet, статьи почтовых списков рассылки. Все это довольно разнородная информация, которая представлена в виде различных, никак несогласованных друг с другом форматов данных. Здесь есть и текстовая информация, и графическая информация, и аудио информация и вообще все, что есть в указанных выше хранилищах. Естественно встает вопрос, как информационно-поисковая система должна со всем этим работать. В традиционных системах есть понятие поискового образа документа - ПОД (Поисковый Образ Документа) - это нечто, что заменяет собой документ и используется при поиске вместо реального документа. Поисковый образ является результатом применения некоторой модели информационного массива документов к реальному массиву. Наиболее популярной моделью является векторная модель, в которой каждому документу приписывается список терминов, наиболее адекватно отражающих его смысл.

Таким образом, первая задача, которою должна решить информационно-поисковая система - это приписывание списка ключевых слов документу или информационному ресурсу. Именно эта процедура и называется индексированием.

Проблема, связанная с индексированием, заключается в том, что приписывание поискового образа документу или информационному ресурсу опирается на представление о словаре, из которого эти термины выбираются, как о фиксированной совокупности терминов. В традиционных системах существовало разбиение на системы с контролируемым словарем и системы со свободным словарем. Контролируемый словарь предполагал ведение некоторой лексической базы данных, добавление терминов в которую производилось администратором системы. Таким образом, все новые документы могли быть заиндексированы только теми терминами, которые были в этой базе данных. Свободный словарь пополнялся автоматически по мере появления новых документов. Однако, на момент актуализации словарь также фиксировался. Актуализация предполагала полную перезагрузку базы данных. В момент этого обновления перегружались сами документы и обновлялся словарь, а после его обновления производилась переиндексация документов. Процедура актуализации занимала достаточно много времени и доступ к системе в момент ее актуализации закрывался.

После того, как ресурсы заиндексированы, т.е. система составила массив поисковых образов документов, начинается построение поискового аппарата системы. Совершенно очевидно, что лобовой просмотр файла или файлов ПОД'ов займет много времени, что абсолютно не приемлемо для интерактивной системы, которой является Web. Для того, чтобы можно было быстро находить информацию в базе данных ПОД'ов строится индекс. Индекс в большинстве систем - система связанных между собой файлов, которая нацелена на быстрый поиск данных по запросу пользователя. Структура и состав индексов различных систем могут отличаться друг от друга и зависят от многих факторов. К этим факторам можно отнести и размер массива поисковых образов, и информационно-поисковый язык системы, и размещения различных компонентов системы и т.п.

Успех информационно-поисковой системы с точки зрения скорости поиска, определяется исключительно архитектурой индекса. Как правило, способ организации этих массивов является "секретом фирмы" и гордостью компании.

4.4.3 Информационно-поисковый язык системы

Однако, индекс - это только часть поискового аппарата, причем не видная глазу пользователя. Второй частью этого аппарата является информационно-поисковый язык. ИПЯ позволяет сформулировать запрос к системе в довольно простой и доходчивой форме. Уже давно осталась позади романтика создания ИПЯ, как естественного языка. Именно этот подход использовался в системе Wais на первых стадиях ее реализации. Если даже пользователю предлагается вводить за-

просы на естественном языке, то это не значит, что система будет осуществлять семантический разбор запроса пользователя. Проза жизни заключается в том, что обычно фраза разбивается на слова, из этого списка удаляются запрещенные и общие слова, иногда производится нормализация лексики, а затем все слова связываются либо логическим AND, либо OR. Таким образом запрос типа:

>Software that is used on Unix Platform будет преобразован в: >Unix AND Platform AND Software

что будет означать примерно следующее: "Найди все документы, в которых слова Unix, Platform и Software встречаются одновременно".

4.4.4 Традиционные информационно-поисковые языки и их модификации

Наиболее распространенным ИПЯ является язык, позволяющий составить логические выражения из набора терминов. При этом используются булевые операторы AND, OR, NOT. Такая схема достаточно проста, и поэтому наиболее широко применяется в современных информационно-поисковых системах. Но еще 20 лет тому назад были хорошо известны и ее недостатки.

Булевый поиск плохо масштабирует выдачу. Оператор AND может очень сильно сократить число документов, которые выдаются на запрос. При этом все будет очень сильно зависеть от того, насколько типичными для базы данных являются поисковые термины. Оператор OR напротив может привести к неоправданно широкому запросу, в котором полезная информация затеряется за информационным шумом. Для успешного применения этого ИПЯ следует хорошо знать лексику системы и ее тематическую направленность. Как правило, для системы с таким ИПЯ создаются специальные документально лексические базы данных со сложными словарями, которые называются тезаурусами и содержат информацию о связи терминов словаря друг с другом.

Модификацией булевого поиска является взвешенный булевый поиск. Идея такого поиска достаточно проста. Считается, что термин описывает содержание документа с какой-то точностью, и эту точность выражают в виде веса термина. При этом взвешивать можно как термины документа, так и термины запроса. Запрос может формулироваться на ИПЯ, описанном выше, но выдача документов при этом будет ранжироваться в зависимости от степени близости запроса и документа. При этом измерение близости строится таким образом, чтобы обычный булевый поиск был бы частным случаем взвешенного булевого поиска.

Языки типа "Like this". При внимательном рассмотрении взвешенного поиска закрадывается естественное желание вообще обойтись без логических коннекторов и измерять близость документа и запроса какими-либо другими критериями. Наиболее простой моделью этого типа является линейная модель индексирования и поиска, когда близость документа и запроса рассматривается как угол между ними. В этом случае высчитывается sin угла, который получают как скалярное произведение двух векторов. В соответствии со значением меры близости происходит ранжирование документов при выдаче ссылок на них пользователю.

Поиск в нечетких множествах. При этом типе поиска весь массив документов описывается как набор нечетких множеств терминов. Каждый термин определяет некую монотонную функцию принадлежности документам документального массива. Когда запрашивается AND, то это интерпретируется как минимум из двух функций, соответствующих терминам запросов, OR - как максимум, NOT - как 1-<значение функции>. В соответствии с полученными значениями результат поиска также ранжируется, как и в случае с поиском по мерам близости.

Следует сразу сказать, что этот метод поиска используется только в исследовательских системах и распространен крайне ограничено.

Пороговые модели. Как было видно из предыдущего изложения, на конечном этапе поиска выборка найденных документов ранжируется. поиск в нечетких множествах приводит к ранжированию всего массива документов в базе данных. Современные информационно-поисковые системы Internet имеют базы данных только индексов, занимающие террабайты. Ранжировать целиком такие массивы - это просто безумная затея. Поэтому применяются пороговые модели, которые задают пороговые значения для документов, выдаваемых пользователю.

Кластерная модель и Вероятностная модель информационного поиска. В кластерной модели может использоваться два подхода. Первый заключается в том, что массив заранее разбивается на

подмножества документов и при поиске высчитывается близость запроса некоторому подмножеству.

При вероятностной модели вычисляется вероятность принадлежности документа классу релевантных запросу документов. При этом используется вероятность принадлежности терминов запроса каждому из документов базы данных.

Коррекция запроса по релевантности. Многие системы применяют механизм коррекции запроса по релевантности. Это означает, что процедура поиска носит интерактивный и итеративный характер. После проведения первичного поиска пользователь отмечает из всего списка найденных документов релевантные. На следующие итерации система расширяет/уточняет запрос пользователя терминами из этих документов и снова выполняет поиск. Так продолжается до тех пор пока пользователь не сочтет, что лучшего результата, чем он уже имеет добиться не удастся. Коррекция запроса по релевантности - это достаточно широко внедренный способ уточнения запросов.

3.6.6. Информационно-поисковые языки Internet

При описании и классификации информационно-поисковых систем ставилась задача проанализировать наиболее популярные и наиболее типичные системы, которыми пользуются в Сети.

Lycos

Как и большинство систем, Lycos дает возможность использовать простой запрос и более изощренный метод поиска. В простом запросе в качестве поискового критерия вводится предложение на естественном языке. Lycos производит нормализацию запроса, удаляя из него так называемые stop-слова, и только после этого приступает к его выполнению. Почти сразу выдается информация о числе документов на каждое слово, а уже позже и список ссылок на формально релевантные документы. В списке напротив каждого документа указывается его мера близости запросу, число слов из запроса, которые попали в документ и оценочная мера близости, которая может быть больше или меньше формально вычисленной. На апрель 1996 года в Lycos не был реализован булевый поиск, такие планы были анонсированы. Последнее предложение подразумевает только то, что нельзя вводить эти операторы в строке вместе с терминами, но использовать логику через систему меню Lycos позволяет. Последнее относится к расширенной форме запроса, который предназначен для использования искушенными пользователями системы, которые уже научились пользоваться этим механизмом.

Таким образом мы видим, что Lycos относится к системе с языком запросов типа "Like this", но предполагается его расширения и на другие способы организации поисковых предписаний.

AltaVista

Наиболее интересным с точки зрения информационно-поискового языка в AltaVista является возможность расширенного поиска. Здесь стоит сразу выделить, что в отличии от многих систем AltaVista поддерживает одноместный оператор NOT. Кроме этого есть еще и оператор NEAR, который реализует возможность контекстного поиска, когда термины должны располагаться рядом в тексте документа. AltaVista разрешает поиск по ключевым фразам, при этом она имеет довольно большой словарь этих фраз. Кроме всего прочего, при поиске в AltaVista можно задать имя поля где должно встретиться слово. Это может быть гипертекстовая ссылка, applet, название образа, заголовок и ряд других полей. К сожалению, подробно процедура ранжирования в документации по системе не описана, но сказано, что ранжирование применяется как при простом поиске, так и при расширенном запросе.

Реально эту систему можно отнести к системе с расширенным булевым поиском.

Yahoo

Данная система появилась в сети одной из первых, и поэтому говорить будем о сегодняшнем состоянии Yahoo, а не о состоянии годовой давности. В настоящее время Yahoo сотрудничает со многими производителями средств информационного поиска и на различных ее серверах используется различное программное обеспечение. На мой взгляд, это самая незатейливая информационная служба, которая сосредоточилась на информации о Web как таковой. ИПЯ Yahoo достаточно прост: все слова следует вводить через пробел и они соединяются либо AND, либо OR. При выдаче не выдается степени соответствия документа запросу, а только подчеркиваются слова из запроса, которые встретились в документе. При этом не производится нормализация лексики и не про-

водится анализ на "общие" слова. Хорошие результаты поиска получаются только тогда, когда пользователь знает, что информация в базе данных Yahoo точно есть. Ранжирование производится по числу терминов запроса в документе.

Yahoo относится к классу простых традиционных систем с ограниченными возможностями поиска.

OpenText

Информационная система OpenText представляет из себя самый коммерциализированный информационный продукт в сети. Все описания больше напоминают рекламу, чем реальное руководство по работе. Система позволяет провести поиск с использованием логических коннекторов, размер запроса ограничен тремя терминами или фразами. В данном случае речь идет о расширенном поиске. При выдаче результатов поиска сообщается степень соответствия документа запросу и размер документа. Система позволяет также улучшить результаты поиска в стиле традиционного булевого поиска.

OpenText можно было бы отнести без сомнения к разряду традиционных информационно-поисковых систем, если бы не механизм ранжирования.

InfoSeek

Система InfoSeek обладает довольно развитым информационно-поисковым языком, который позволяет не просто указывать какие термины должны встречаться в документах, но и своеобразно взвешивать их. Достигается это при помощи специальных знаков "+" - термин обязан быть в документе, "-" - термин обязан отсутствовать в документе. Кроме этого InfoSeek позволяет проводит то, что называется контекстным поиском. Это значит, что используя специальную форму запроса можно потребовать последовательной совместной встречаемости слов. Кроме этого можно указать, что некоторые слова должны совместно встречаться не только в одном документе, а даже в отдельном параграфе или заголовке. Есть возможность и указания ключевых фраз. Ключевая фраза от последовательной встречаемости отличается тем, что фраза всегда ищется как единое целое, а при последовательной встречаемости слова могут стоять рядом, но в произвольном порядке. Ранжирование при выдаче осуществляется по числу терминов запроса в документе, по числу фраз запроса в документе, за вычетом общих слов. Все эти факторы используются как вложенные процедуры.

Подводя краткое резюме можно сказать, что InfoSeek относится к традиционным системам с элементом взвешивания терминов при поиске.

WAIS

WAIS является одной из наиболее изощренных поисковых систем Internet. В отличии от многих поисковых машин, ИПЯ системы позволяет строить не только вложенные булевые запросы, считать формальную релевантность по различным мерам близости, взвешивать термины запроса и документа, но и осуществлять коррекцию запроса по релевантности. Система также позволяет использовать усечение терминов, разбиение документов на поля и ведение распределенных индексов. Не случайно именно эта система была выбрана в качестве основной поисковой машины для реализации энциклопедии "Британика" на Internet.

3.6.7. Интерфейс системы

Важным фактором является вид представления информации в программе-интерфейсе. При этом различают два типа интерфейсных страниц: страницы запросов и страницы результатов поиска.

При составлении запроса к системе используют либо меню-ориентированный подход, либо командную строку. Меню-ориентированный подход позволяет ввести список терминов, обычно через пробел, и выбрать тип логической связи между ними. Логическая связь распространяется на все термины. На нашей схеме (рисунок 3.41) есть так называемые сохраненные запросы пользователя. В большинстве систем это просто фраза на ИПЯ, которую можно расширить за счет добавления новых терминов и логических операторов. Но это только один тип использования сохраненных запросов. В традиционных системах это называется расширением или уточнением запроса, в зависимости от того, что получаем в результате преобразования запроса: увеличение размера выборки или ее сокращение. При этом традиционная система хранит не запрос как таковой, а резуль-

тат поиска, т.е. список идентификаторов документов, который объединяется/пересекается со списком полученным при поиске документов по новым терминам. К сожалению, сохранение списка идентификаторов найденных документов в World Wide Web не практикуется. Вызвано это особенностью протоколов взаимодействия программы-клиента и сервера системы, которые не поддерживают сеансовый режим работы.

Как стало уже понятно из выше изложенного, результат поиска в базе данных ИПС - это список указателей на удовлетворяющие запросу документы. Различные системы представляют этот список по-разному. В некоторых системах выдается только список ссылок, а в таких системах как Lycos, AltaVista, Yahoo кроме ссылок дается еще и краткое описание, которое заимствуется либо из заголовков, либо из тела самого документа. Кроме этого система сообщает на сколько найденный документ соответствует запросу. В Yahoo, например, сообщается сколько терминов запроса содержится в поисковом образе документа и в соответствии с этим ранжируется результат поиска. В Lycos выдается мера соответствия документа запросу и ранжирование производится по этому параметру. Обычно пользователь имеет возможность уточнить запрос.

При обзоре интерфейсов и средств поиска нельзя пройти мимо процедуры коррекции запросов по релевантности[7]. Релевантность - это мера соответствия найденного системой документа потребности пользователя. Различают формальную релевантность и реальную. Формальная - это та, что вычисляет система и на основании чего ранжируется выборка найденных документов. Реальная - это та, как сам пользователь оценивает найденные документы. Некоторые системы имеют для этого специальное поле[6], где пользователь может отметить документ как релевантный. При следующей поисковой итерации запрос расширяется терминами этого документа. И выдача снова ранжируется. Так происходит до тех пор, пока результат не стабилизируется. Это означает, что ничего лучше, чем полученная выборка, от данной системы не добьешься.

Кроме ссылок на документы в списке, полученном пользователем, могут оказаться ссылки на части документов или на их поля. Это происходит при наличии ссылок типа http://host/path#mark или ссылок по схеме WAIS. Возможны ссылки и на скрипты, но обычно такие ссылки роботы пропускают и система не индексирует. Если с http-ссылками все более или менее понятно, то ссылки WAIS - это гораздо более сложные объекты. Дело в том, что WAIS реализует архитектуру распределенной информационно-поисковой системы. Это значит, что одна ИПС, например, Lycos строит поисковый аппарат над поисковым аппаратом другой системы - WAIS. При этом серверы WAIS имеют свои собственные локальные базы данных. При загрузке документов в WAIS администратор может описать структуру документов, т.е. разбить их на поля, и хранить документы как один файл. индекс WAIS будет ссылаться на отдельные документы и их поля как на самостоятельные единицы хранения. В этом случае программа просмотра ресурсов Internet должна уметь работать с протоколом WAIS, чтобы получить доступ к этим документам.

Администрирование сетей Windows

Краткое знакомство со службой каталогов Windows 2000

Служба каталогов используется для уникальной идентификации пользователей и ресурсов в сети. Для работы службы каталогов Windows 2000 применяет Active Directory. Важно понимать основную цель Active Directory и ее ключевые возможности.

Что такое служба каталогов

Каталог (Directory) — сохраненный набор информации об объектах, связанных друг с другом некоторым способом. Например, в телефонном справочнике хранятся имена объектов и соответствующие им телефонные номера. Телефонный справочник также может содержать адрес или другую информацию об объекте.

В распределенных компьютерных системах или глобальных сетях типа Интернета существует множество объектов, например файловые серверы, принтеры, службы факсов, приложения, базы данных и пользователи, которые находят и используют эти объекты.

Необходимо, чтобы администраторы имели возможность управлять этими объектами. Служба каталогов централизованно хранит всю информацию, требуемую для использования и управления этими объектами, упрощая процесс поиска и управления данными ресурсами.

В данном курсе термины каталог и служба каталогов относятся к каталогам, расположенным в глобальных и частных сетях.

Каталог предоставляет средство хранения информации, относящейся к сетевым ресурсам, облегчая их поиск и управление ими.

Служба каталогов — сетевая служба, которая идентифицирует все ресурсы сети и делает их доступными пользователям. Служба каталогов отличается от каталога тем, что хотя они оба являются источниками информации, служба делает ее доступной для пользователей.

Служба каталогов работает как главный коммутатор сетевой ОС. Она управляет идентификацией и отношениями между распределенными ресурсами и позволяет им работать вместе. Ввиду поддержки службой каталогов этих фундаментальных функций ОС, они должны быть тесно связаны с механизмами управления и безопасности ОС для обеспечения целостности и защищенности сети. Они также необходимы для определения и поддержания инфраструктуры сети организации, администрирования системы и контроля активности пользователей информационной службы компании.

Назначение службы каталогов

Служба каталога предоставляет средства организации и упрощения доступа к ресурсам сетевой компьютерной системы. Пользователи и администраторы могут не знать точное название необходимых им объектов. Им достаточно знать один или несколько атрибутов рассматриваемых объектов. Пользователи обращаются к службе каталогов для запроса списка объектов, отвечающих известным атрибутам. Например, в ответ на запрос «Найти все цветные принтеры на третьем этаже» каталог выдаст сведения обо всех объектах цветных принтеров с атрибутами «цветной» и «третий этаж» (или у которых атрибут местоположения равен «третий этаж»). Служба каталогов позволяет искать объект по одному или нескольким его атрибутам.

Служба каталогов выполняет и другие функции:

- назначение безопасности для защиты объектов БД от внешних вторжений или внутренних пользователей, не имеющих доступа к данным объектам;
- распространение каталога на множество компьютеров сети;
- дублирование каталога для предоставления доступа большему количеству пользователей и отказоустойчивости;
- деление каталога на несколько хранилищ, расположенных на разных компьютерах сети. Это увеличивает доступное для каталога пространство в целом и позволяет хранить больше объектов.

Служба каталогов является как инструментом администрирования, так и инструментом пользователя. При расширении сети приходится управлять все большим количеством объектов ресурсов, и наличие службы каталога становится насущной необходимостью.

Возможности службы каталогов Windows 2000

Active Directory — это служба каталогов в Windows 2000 Server. Active Directory содержит каталог, в котором хранится информация о сетевых ресурсах и службы, предоставляющие доступ к этой информации. Ресурсы, хранящиеся в каталоге, такие, как данные, сведения о принтерах, серверах, базах данных, группах, службах, компьютерах, политике безопасности, — называются объектами (object).

Active Directory встроена в Windows 2000 Server и обеспечивает:

- упрощенное администрирование;
- масштабируемость;
- поддержку открытых стандартов;
- поддержку стандартных форматов имен.

Упрощенное администрирование

Active Directory иерархически упорядочивает ресурсы в домене (domain) — логическом объединении серверов и других сетевых ресурсов в единое имя домена. Домен является основной единицей репликации и безопасности в сети Windows 2000.

Каждый домен включает один или несколько контроллеров домена. Контроллер домена (domain controller) — компьютер под управлением Windows 2000 Server, обеспечивающий доступ

пользователей в сеть: вход в систему, проверку подлинности и доступ к каталогу и общим ресурсам. Для простоты администрирования все контроллеры домена равнозначны. Изменения, сделанные на любом из них, реплицируются на остальные контроллеры в домене.

Active Directory дополнительно упрощает администрирование, предоставляя единую точку администрирования всех объектов сети. Благодаря этому администратор может, войдя в систему на одном компьютере, управлять объектами, расположенными на любом компьютере в сети.

Масштабируемость

В Active Directory каталог помещает информацию в разделы, позволяющие хранить множество объектов. В результате каталог расширяется с ростом организации. Это позволяет переходить от небольших установок с несколькими сотнями объектов к большим с миллионами объектов.

Поддержка открытых стандартов

Active Directory соответствует концепции пространства имен Интернета в части службы каталогов Windows 2000. Это позволяет унифицировать и управлять множеством пространств имен, существующих в настоящее время в разнородном программном и аппаратном окружении корпоративных сетей. В качестве системы именования Active Directory использует DNS и способен обмениваться информацией с любым приложением или каталогом, использующим LDAP или протокол передачи гипертекста (HTTP).

DNS

Поскольку Active Directory для доменного именования и службы поиска использует DNS, имена доменов Windows 2000 также являются именами DNS. Windows 2000 Server применяет динамическую DNS (DDNS), позволяющую клиентам с динамически назначенными адресами напрямую регистрироваться на сервере с работающей службой DNS и динамически обновлять таблицу DNS. В однородной среде DDNS устраняет потребность в других службах именования Интернета, например в службе имен Интернета для Windows (Windows Internet Name Service, WINS).

Поддержка LDAP и HTTP

Active Directory отвечает стандартам Интернета и напрямую поддерживает LDAP и HTTP. LDAP — версия протокола доступа к каталогу X.500, разработан в качестве упрощенной альтернативы протокола доступа к каталогам (Directory Access Protocol, DAP). Active Directory поддерживает обе версии LDAP: 2 и 3. HTTP является стандартным протоколом для отображения страниц во всемирной сети Интернет. Пользователи могут просматривать каждый объект в Active Directory, как HTML-страницу в обозревателе Web, пользуясь при запросах и просмотре объектов Active Directory всеми преимуществами знакомой модели обозревателя Web.

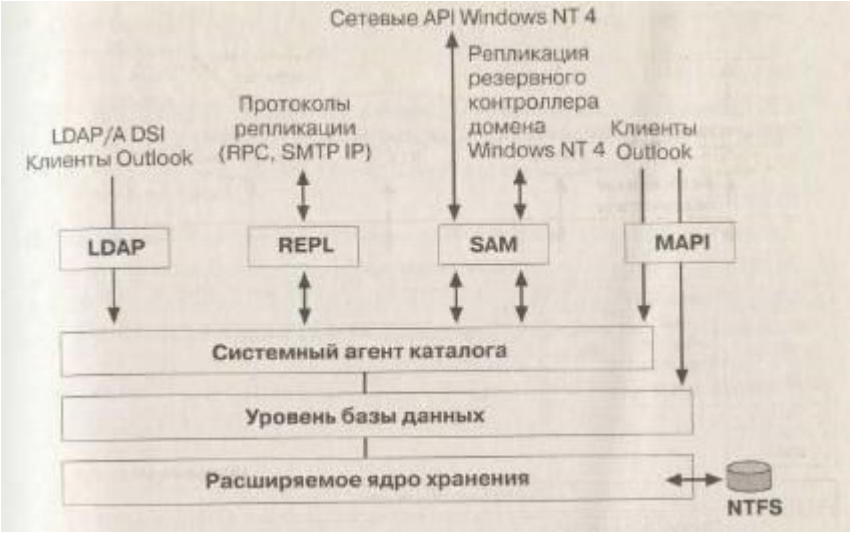
Для обмена информацией между каталогами и приложениями Active Directory использует LDAP.

Active Directory поддерживает несколько общих форматов имен, следовательно, для обращения к Active Directory пользователи могут выбрать наиболее привычный формат.

Active Directory работает в безопасной подсистеме в пользовательском режиме. Тесная взаимосвязь службы каталога и подсистемы безопасности является основой для работы распределенных систем Windows 2000. Доступ к любому объекту каталога требует сначала удостоверения личности (проверки подлинности), а затем и проверки разрешений Доступа (авторизации), которая выполняется компонентами подсистемы безопасности вместе с эталонным монитором безопасности.

Архитектура Active Directory

Функциональную структуру Active Directory можно представить в виде многоуровневой архитектуры, в которой уровни являются процессами, предоставляющими клиентским приложениям доступ к службе каталога. Active Directory состоит из трех уровней служб и нескольких интерфейсов и протоколов, совместно работающих для предоставления доступа к службе каталога. Три уровня служб охватывают различные типы информации, необходимой для поиска записей в БД каталога. Выше уровней служб в этой архитектуре находятся протоколы и API-интерфейсы, осуществляющие связь между клиентами и службой каталога.




На рис. изображены уровни службы Active Directory и соответствующие им интерфейсы и протоколы. Стрелки показывают, как различные клиенты получают при помощи интерфейсов доступ к Active Directory.

· Системный агент каталога (Directory System Agent, DSA). Выстраивает иерархию родительско-дочерних отношений, хранящихся в каталоге. Предоставляет API-интерфейсы для вызовов доступа к каталогу.

· Уровень БД. Предоставляет уровень абстрагирования между приложениями и БД. Вызовы из приложений никогда не выполняются напрямую к БД, а только через уровень БД.

· Расширяемое ядро хранения. Напрямую взаимодействует с конкретными записями в хранилище каталога на основе атрибута относительного составного имени объекта.

· Хранилище данных (файл БД NTDS.DIT). Управляется при помощи расширяемого механизма хранения БД, расположенного в папке \Winnt\NTDS на контроллере домена.

· Клиенты получают доступ к Active Directory, используя механизмы, поддерживаемые DSA.

· LDAP/ADSI. Клиенты, поддерживающие LDAP, используют его для связи с DSA. Active Directory поддерживает LDAP версии 2 (описан в RFC 1777). Клиенты Windows 2000, Windows 98 и Windows 95 с установленными клиентскими компонентами Active Directory для связи с DSA используют LDAP версии 3.

· API-интерфейс обмена сообщениями (Messaging API, MAPI, Messaging Application Programming Interface). Традиционные клиенты MAPI, например Microsoft Outlook, подключаются к DSA, используя интерфейс поставщика адресной книги MAPI RPC(Remote Procedure Call)

· Диспетчер учетных записей безопасности (Security Accounts Manager, SAM). Клиенты Windows NT версии 4.0 или более ранней используют интерфейс SAM для связи с DSA. Репликация с резервных контроллеров в домене смешанного режима также выполняется через интерфейс SAM.

· Репликация (REPL). При репликации каталога, агенты DSA взаимодействуют друг с другом, используя патентованный интерфейс RPC.

Active Directory

Средства Active Directory позволят вам спроектировать структуру каталога так, как это нужно вашей организации.

Объекты Active Directory

Active Directory хранит информацию о сетевых ресурсах. Как уже было сказано эти ресурсы, например данные пользователей, описания принтеров, серверов, баз данных, групп, компьютеров и политик безопасности, и называются объектами (object).

Объект — это отдельный именованный набор атрибутов, которыми представлен сетевой ресурс. Атрибуты (attribute) объекта являются его характеристиками в каталоге. Например, атрибуты

учетной записи пользователя (user account) могут включать в себя его имя и фамилию, отдел, а также адрес электронной почты

Рис. 2-1. Объекты Active Directory и их атрибуты

В Active Directory объекты могут быть организованы в классы, то есть в логические группы. Примером класса является объединение объектов, представляющих учетные записи пользователей, группы, компьютеры, домены или организационные подразделения (ОП).

Примечание Объекты, которые способны содержать другие объекты, называются контейнерами (container). Например, домен — это контейнерный объект, который может содержать пользователей, компьютеры и другие объекты.

Какие именно объекты могут храниться в Active Directory, определяется ее схемой.

Схема Active Directory

Схема Active Directory — это список определений (definitions), задающих виды объектов, которые могут храниться в Active Directory, и типы сведений о них. Сами эти определения также хранятся в виде объектов, так что Active Directory управляем ими посредством тех же операций, которые используются и для остальных объектов в Active Directory.

В схеме существуют два типа определений: атрибуты и классы. Также они называются объектами схемы (schema objects) или метаданными (metadata).

Атрибуты определяются отдельно от классов. Каждый атрибут определяется только один раз, при этом его разрешается применять в нескольких классах. Например, атрибут Description используется во многих классах, однако определен он в схеме только однажды, что обеспечивает ее целостность.

Классы, также называемые классами объектов (object classes), описывают, какие объекты Active Directory можно создавать. Каждый класс является совокупностью атрибутов. При создании объекта атрибуты сохраняют описывающую его информацию. Например, в число атрибутов класса User входят Network Address, Home Directory и пр. Каждый объект в Active Directory — это экземпляр класса объектов.

В Windows 2000 Server встроен набор базовых классов и атрибутов.

Определяя новые классы и новые атрибуты для уже существующих классов, опытные разработчики и сетевые администраторы могут динамически расширить схему. Например, если Вам нужно хранить информацию о пользователях, не определенную в схеме, можно расширить схему для класса Users. Однако такое расширение схемы — достаточно сложная операция с возможными серьезными последствиями.

Компоненты Active Directory

Active Directory использует компоненты для построения структуры каталога, отвечающей требованиям вашей организации. Логическую структуру организации представляют домены, организационные подразделения, деревья, леса. Физическая структура организации представлена узлами (физическими подсетями) и контроллерами доменов. В Active Directory логическая структура полностью отделена от физической.

Логическая структура

В Active Directory ресурсы организованы в логическую структуру, отражающую структуру вашей организации. Это позволяет находить ресурс по его имени, а не физическому расположе-

нию. Благодаря логическому объединению ресурсов в Active Directory физическая 1 структура сети не важна для пользователей.

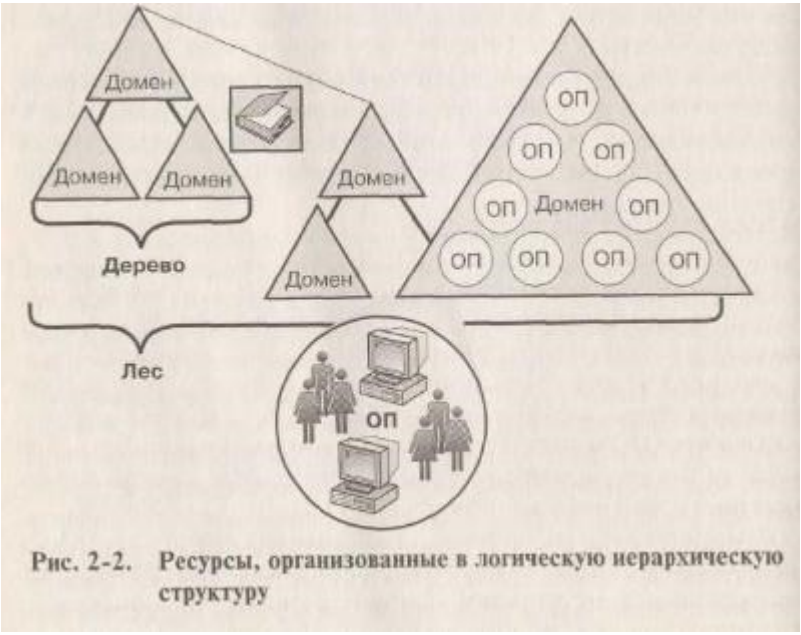



Рис. 2-2. Ресурсы, организованные в логическую иерархическую структуру

Домен

Основным элементом логической структуры в Active Directory является домен, способный содержать миллионы объектов. В домене хранятся объекты, которые считаются «интересными» для сети. «Интересные» объекты — это то, в чем члены сетевого сообщества нуждаются для своей работы: принтеры, документы, адреса электронной почты, базы данных, пользователи, распределенные компоненты и прочие ресурсы. Active Directory может состоять из одного или более доменов.

Объединение объектов в один или более доменов позволяет отразить в сети организационную структуру компании. Общие характеристики доменов таковы:

- все сетевые объекты существуют в пределах домена, а каждый домен хранит информацию только о тех объектах, которые содержит. Теоретически каталог домена может содержать до 10 миллионов объектов, но фактически — это около 1 миллиона объектов на домен;
- домен обеспечивает безопасность. В списках управления доступом(access control lists, ACL) определяется доступ к объектам домена. В них заданы разрешения для пользователей, которые могут получить доступ к объекту, и указан тип этого доступа. В Windows 2000 объекты включают файлы, папки, общие ресурсы, принтеры и другие объекты Active Directory. В разных доменах никакие параметры безопасности, например административные права, политики безопасности, списки управления доступом, не пересекаются между собой. Администратор домена имеет абсолютное право устанавливать политики только внутри данного домена.

Организационное подразделение (ОП) — это контейнер, используемый для объединения объектов домена в логические административные группы, отражающие деятельность или бизнес-структуру организации. Организационное подразделение (ОП) может содержать объекты, например учетные записи пользователей, группы, компьютеры, принтеры, приложения, совместно используемые файловые ресурсы, а также другие ОП из того же домена. Иерархия ОП одного домена не зависит от иерархической структуры другого домена, а каждый домен может иметь свою собственную структуру ОП.

ОП представляют собой средства выполнения административных задач, поскольку являются объектами наименьшего масштаба, которым разрешается делегировать административные полномочия, то есть администрирование пользователей и ресурсов.

Дерево (tree) — это группа, или иерархически упорядоченная совокупность из одного или более доменов Windows 2000, созданная путем добавления одного или более дочерних доменов к уже существующему родительскому домену. Все домены в дереве используют связанное пространство имен и иерархическую структуру именования.

Характеристики деревьев таковы:

• согласно стандартам доменной системы имен (Domain Name System, DNS), доменным именем дочернего домена будет объединение его относительного имени и имени родительского домена.

• все домены в пределах одного дерева совместно используют общую схему, которая служит формальным определением всех типов объектов, находящихся в Вашем распоряжении при развертывании Active Directory;

• все домены в пределах одного дерева совместно используют общий глобальный каталог, который служит центральным хранилищем информации об объектах в дереве.

Лес (forest) — это группа, или иерархически упорядоченная совокупность, из одного или более отдельных и полностью независимых доменных деревьев. Деревья обладают следующими характеристиками:

• у всех деревьев в лесе общая схема;

• у всех деревьев в лесе разные структуры именования, соответствующие своим доменам;

• все домены в лесе используют общий глобальный каталог;

• домены в лесе функционируют независимо друг от друга, однако лес допускает обмен данными в масштабе всей организации;

• между доменами и деревьями доменов существуют двусторонние доверительные отношения.

Физическая структура

Физические компоненты Active Directory — это узлы и контроллеры домена. Эти компоненты применяются для разработки структуры каталога, отражающей физическую структуру вашей организации.

Сайт

Сайт (site) — это объединение одной или более подсетей IP для создания максимально возможного ограничения сетевого трафика, высоконадежным каналом связи с высокой пропускной способностью. Как правило, границы узла совпадают с границами ЛВС. Когда Вы группируете подсети, следует объединять только те из них, которые между собой связаны быстрыми, дешевыми и надежными сетевыми соединениями. В Active Directory сайты не являются частью пространства имен. Просматривая логическое пространство имен, вы увидите, что компьютеры и пользователи сгруппированы в домены и ОП, а не в сайты. Сайты содержат лишь объекты компьютеров и соединений, нужные для настройки межсайтовой репликации.

Контроллеры домена

Контроллер домена — это компьютер с Windows 2000 Server, хранящий реплику каталога домена (локальную БД домена). Поскольку в домене может быть несколько контроллеров домена, все они хранят полную копию той части каталога, которая относится к их домену.

Концепции работы Active Directory

Вместе с Active Directory введено несколько новых понятий, например, глобальный каталог, репликация, доверительные отношения, пространство имен DNS и правила наименования. Важно понимать их значение применительно к Active Directory.

Глобальный каталог (global catalog) — это центральное хранилище информации об объектах в дереве или лесе (рис. 2-6). По умолчанию глобальный каталог автоматически создается на первом контроллере домена в лесе, и этот контроллер становится сервером глобального каталога (global catalog server). Он хранит полную реплику атрибутов всех объектов в своем домене, а также частичную реплику атрибутов всех объектов для каждого домена в лесе. Эта частичная реплика хранит те атрибуты, которые чаще других нужны при поиске (например, по имени или фамилии пользователя, по регистрационному имени пользователя и т. д.). Атрибуты объекта в глобальном каталоге наследуют исходные разрешения доступа из тех доменов, откуда они были реплицированы, и таким образом, в глобальном каталоге обеспечивается безопасность данных.

Глобальный каталог выполняет две важные функции: 1.обеспечивает регистрацию в сети, предоставляя контроллеру домена информацию о членстве в группах;

2.обеспечивает поиск информации в каталоге независимо от расположения данных.

Когда пользователь регистрируется в сети, глобальный каталог предоставляет контроллеру домена, который обрабатывает информацию о процессе регистрации в сети, полные данные о членстве учетной записи в группах. Если в домене только один контроллер, сервер глобального каталога и контроллер домена — это один и тот же сервер. Если же в сети несколько контроллеров домена, то глобальный каталог располагается на том из них, который сконфигурирован для этой роли. Если при попытке регистрации в сети глобальный каталог недоступен, то пользователю разрешается зарегистрироваться, лишь на локальном компьютере.


Рис. 2-6. Глобальный каталог — центральное хранилище информации

Глобальный каталог позволяет максимально быстро и с минимальным сетевым трафиком отвечать на запросы программ и пользователей об объектах, расположенных в любом месте леса или дерева доменов. Глобальный каталог может разрешить запрос в том же домене, в котором этот запрос был инициирован, так как информация обо всех объектах всех доменов в лесе содержится в едином глобальном каталоге. Поэтому поиск информации в каталоге не вызывает лишнего трафика между доменами.

В качестве сервера глобального каталога вы можете по своему выбору настроить любой контроллер домена либо дополнительно назначить на эту роль другие контроллеры домена. Выбирая сервер глобального каталога, надо учесть, справится ли сеть с трафиком репликации и запросов. Впрочем, дополнительные серверы позволят ускорить время отклика на запросы пользователей. Рекомендуется, чтобы каждый крупный сайт предприятия имел собственный сервер глобального каталога.

Репликация

Необходимо, чтобы с любого компьютера в дереве доменов или лесе пользователи и службы могли все время получать доступ к информации в каталоге. Репликация позволяет отражать изменения в одном контроллере домена на остальных контроллерах в домене. Информация каталога реплицируется на контроллеры домена как в пределах узлов, так и между ними.

Виды реплицируемой информации

Хранимая в каталоге информация делится на три категории, которые называются разделами каталога (directory partition). Раздел каталога служит объектом репликации. В каждом каталоге содержится следующая информация:

• информация о схеме — определяет, какие объекты разрешается создавать в каталоге и какие у них могут быть атрибуты;

• информация о конфигурации — описывает логическую структуру развернутой сети, например структуру домена или топологию репликации. Эта информация является общей для всех доменов в дереве или лесе;

• данные домена — описывают все объекты в домене. Эти данные относятся только к одному определенному домену. Подмножество свойств всех объектов во всех доменах хранится в глобальном каталоге для поиска информации в дереве доменов или лесе.

Схема и конфигурация реплицируются на все контроллеры домена в дереве или лесе. Все данные определенного домена реплицируются на каждый контроллер именно этого домена. Все объекты каждого домена, а также часть свойств всех объектов в лесе реплицируются в глобальный каталог.

Контроллер домена хранит и реплицирует: информацию о схеме дерева доменов или леса; информацию о конфигурации всех доменов в дереве или лесе; все объекты и их свойства для своего домена. Эти данные реплицируются на все дополнительные контроллеры в домене. Часть всех свойств объектов домена реплицируется в глобальный каталог для организации поиска информации. Глобальный каталог хранит и реплицирует:

- информацию о схеме в лесе;
- информацию о конфигурации всех доменов в лесе;
- часть свойств всех объектов каталога в лесе (реплицируется только между серверами глобального каталога);
- все объекты каталога и все их свойства для того домена, в котором расположен глобальный каталог.

Как работает репликация

Active Directory реплицирует информацию в пределах сайта чаще, чем между сайтами, сопоставляя необходимость в обновленной информации каталога с ограничениями по пропускной способности сети.

В пределах сайта Active Directory автоматически создает топологию репликации между контроллерами одного домена с использованием кольцевой структуры. Топология определяет путь передачи обновлений каталога между контроллерами домена до тех пор, пока обновления не будут переданы на все контроллеры домена.

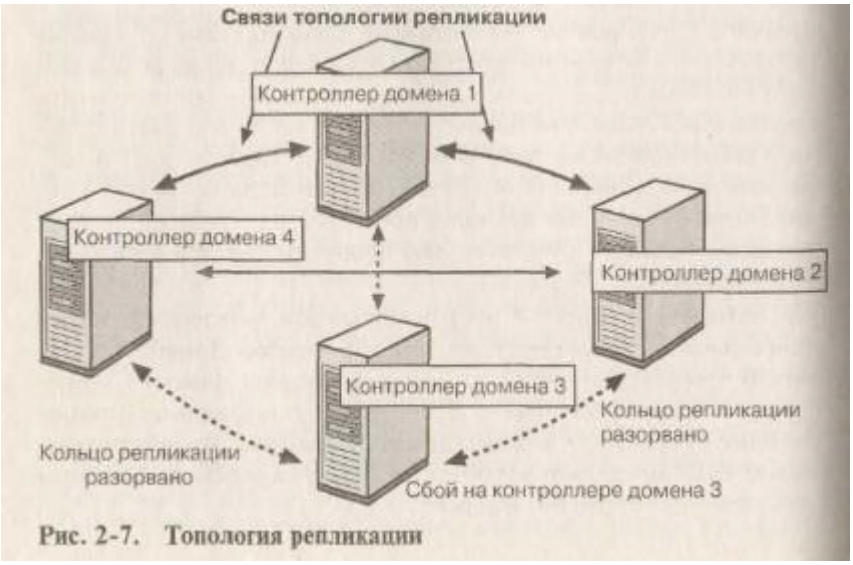


**Рис. 2-7. Топология репликации**

Кольцевая структура обеспечивает существование минимум двух путей репликации от одного контроллера домена до другого, и если один контроллер домена временно становится недоступен, то репликация на остальные контроллеры домена все равно продолжится.

Дабы убедиться, что топология репликации все еще эффективна, Active Directory периодически ее анализирует. Если вы добавите или уберете контроллер домена из сети или узла, то Active Directory соответственно изменит топологию.

Репликация между сайтами

Для обеспечения репликации между узлами нужно представить сетевые соединения в виде связей сайтов (site link). Active Directory использует информацию о сетевых соединениях для создания объектов-соединений, что обеспечивает эффективную репликацию и отказоустойчивость.

Вы должны предоставить информацию о применяемом для репликации протоколе, стоимости связи сайтов, о времени доступности связи и о том, как часто она будет использоваться. Исхо-

дя из этого, Active Directory определит, как связать сайты для репликации. Лучше выполнять репликацию в то время, когда сетевой трафик минимален.

Доверительные отношения

Доверительное отношение (trust realtionship) — это такая связь между двумя доменами, при которой доверяющий домен признает регистрацию в сети в доверяемом домене. Active Directory поддерживает две формы доверительных отношений.

Неявные двусторонние транзитивные доверительные отношения (implicit two-way transitive trust). Это отношения между родительским и дочерним доменами в дереве и между доменами верхнего Уровня в лесе. Они определены по умолчанию, то есть доверительные отношения между доменами в дереве устанавливаются и поддерживаются неявно (автоматически). Транзитивные доверительные отношения — это функция протокола идентификации Kerberos, по которому в Windows 2000 проводится авторизация и регистрация в сети.

Как показано на рис. 2-8, транзитивные доверительные отношения означают следующее: если Домен А доверяет Домену В, а Домен В доверяет Домену С, то Домен А доверяет Домену С. В результате присоединенный к дереву домен устанавливает доверительные отношения с каждым доменом в дереве. Эти доверительные отношения делают все объекты в доменах дерева доступными Для всех других доменов в дереве.

Транзитивные доверительные отношения между доменами устраняют необходимость в междоменных доверительных учетных записях. Домены одного дерева автоматически устанавливают с родительским доменом двусторонние транзитивные доверительные отношения. Благодаря этому пользователи из одного домена могут получить доступ к ресурсам любого другого домена в дереве (при условии, что им разрешен доступ к этим ресурсам).


**Рис. 2-8. Два вида доверительных отношений в Active Directory**

Явные односторонние нетранзитивные доверительные отношения (explicit one-way nontransitive trust). Это отношения между доменами, которые не являются частью одного дерева. Нетранзитивные доверительные отношения ограничены отношениями двух доменов и не распространяются ни на какие другие домены в лесе. В большинстве случаев вы сами можете явно (вручную) создать нетранзитивные доверительные отношения. Так, на рис. 2-8 показаны односторонние транзитивные доверительные отношения, в которых Домен С доверяет Домену 1, так что пользователи в Домене 1 могут получить доступ к ресурсам в Домене С. Явные односторонние нетранзитивные доверительные отношения — это единственно возможные отношения между:

- доменом Windows 2000 и доменом Windows NT;
- доменом Windows 2000 в одном лесе и доменом Windows 2000 в другом лесе;
- доменом Windows 2000 и сферой (realm) MIT Kerberos V5, что позволяет клиентам из сферы Kerberos регистрироваться в домене Active Directory для получения доступа к сетевым ресурсам.

**Групповая политика**

Групповая политика (group policy) представляет собой набор конфигурационных параметров компьютера и пользовательских параметров. Она позволяет определить программы, доступные

пользователям, приложения, значки которых отображаются на рабочем столе, элементы меню Start (Пуск), а также функциональность компьютера.

Объекты групповой политики

Чтобы создать конфигурацию рабочего стола для некоторой группы пользователей, вы создаете объекты групповой политики (ОГП) — наборы параметров политики. На каждом компьютере с Windows 2000 имеется один локальный (local) ОГП; кроме того, на компьютер может распространяться действие неограниченного числа нелокальных (nonlocal) ОГП, основанных на службе каталогов Active Directory. Локальный ОГП хранится на компьютере независимо от того, работает ли последний в сети и есть ли сведения о нем в Active Directory.

Тем не менее, поскольку нелокальные ОГП могут перекрывать пара метры локального ОГП, в среде Active Directory эти параметры меньше всего влияют на конфигурацию рабочего стола. В изолированной среде (или в сети без контроллера домена Windows 2000) параметр локального ОГП приоритетнее, поскольку нелокальные ОГП не могут их перекрыть.

Нелокальные ОГП связаны с объектами Active Directory (сайтами доменами или ОП), и их действие может распространяться на компьютеры или пользователей. Для работы с нелокальными ОГП вам потребуется контроллер домена Windows 2000. В Active Directory правила из нелокальных ОГП суммируются и применяются в соответствии с иерархией: от более крупных группировок (от сайта) к малым (к подразделению).

Параметры групповой политики

Хранятся в ОГП и определяют конфигурацию рабочего стола Пользователя. Существует два вида параметров групповой политики: конфигурационные параметры компьютера и пользовательские параметры.

Конфигурационные параметры компьютера (computer configuration settings) служат для настройки политик, действие которых распространяется на компьютеры независимо от того, какой пользователь входит в систему; они применяются при инициализации системы.

Пользовательские параметры служат для настройки политик, распространяющихся на пользователей, независимо от компьютеров, на которых те регистрируются; они применяются при регистрации пользователя на компьютере.

Для настройки конфигурационных и пользовательских параметров используются узлы Software Settings (Конфигурация программ) Windows Settings (Конфигурация Windows) и Administrative Templates (Административные шаблоны) оснастки Group Policy.

Узел Software Settings

При настройке конфигурационных параметров компьютера и пользовательских параметров по умолчанию этот узел содержит лишь подузел Software Installation (Установка программ), который позволяет определить порядок установки и поддержки приложений в вашей организации. Кроме того, в этот подузел независимые разработчики ПО могут добавлять собственные параметры.

Вы управляете приложением из ОГП, который, в свою очередь, связан с определенным контейнером Active Directory — сайтом, доменом или ОП. Для управления приложением его можно назначить или опубликовать. Назначьте приложение компьютеру, если хотите, чтобы оно было доступно всем пользователям или компьютерам, управляемым данным ОГП. Если вам необходимо предоставлять пользователям, управляемым ОГП, какое-либо приложение по запросу, опубликуйте его. Опубликовать приложение для компьютеров нельзя.

Узел Windows Settings

При настройке конфигурационных параметров компьютера и пользовательских параметров этот узел содержит подузлы Scripts (Сценарии) и Security Settings (Параметры безопасности)

Узел Scripts позволяет определить сценарии запуска/выключения компьютера и сценарии входа в систему/завершения сеанса работы. Если компьютеру назначено несколько сценариев запуска/выключения и входа в систему/завершения сеанса работы, Windows 2000 выполняет их по порядку. При выключении компьютера Windows 2000 обрабатывает сценарии завершения сеанса работы и затем — сценарии выключения системы.

Администраторы могут использовать любой удобный для них язык сценариев ActiveX, в том числе VBScript, JScript, Perl и пакетные файлы MS-DOS (с расширениями .bat и .cmd).

Узел Security Settings (Параметры безопасности) позволяет администратору вручную настроить уровни безопасности для локальных и нелокальных ОГП. Это делается после или вместо настройки системы защиты компьютера с применением шаблона безопасности.

При конфигурировании пользовательских параметров узел Windows Settings также включает подузлы Internet Explorer Maintenance (Поддержка Internet Explorer), Remote Installation Services (Службы Удаленной установки) и Folder Redirection (Перенаправление папки).

Узел Internet Explorer Maintenance позволяет администрировать и настраивать Microsoft Internet Explorer на компьютерах с Windows 2000.

Службы Remote Installation Services управляют процессом удаленной Установки ОС. Кроме того, эти службы можно использовать для предоставления заказных пакетов клиентам Active Directory с операционными системами, отличными от Windows 2000

Узел Folder Redirection позволяет перенаправлять специальные папки Windows 2000 — My Documents (Мои документы), Application Data, Desktop (Рабочий стол) и меню Start (Главное меню) - из исходной папки, заданной в профиле пользователя, в альтернативное место в сети, откуда этими папками можно управлять централизованно.

Узел Administrative Templates

При настройке конфигурационных параметров компьютера и пользовательских параметров этот узел содержит все параметры политики, хранящиеся в реестре, в том числе параметры из подузлов Windows Components (Компоненты Windows), System (Система) и Network (Сеть).

Узел Windows Components позволяет администрировать компоненты Windows 2000, включая NetMeeting, Internet Explorer, Windows Explorer (Проводник), Microsoft Management Console (Консоль управления Microsoft), Task Scheduler (Планировщик заданий) и Windows Installer (Установщик Windows).

Узел System применяется для управления функциями входа в систему и завершения сеанса работы, а также для управления самой групповой политикой.

Узел Network содержит подузлы Offline Files (Автономные файлы) и Network and Dial-Up Connections (Сеть и удаленный доступ к сети).

При настройке конфигурационных параметров компьютера узел Administrative Templates содержит также подузел Printers (Принтеры)-Кроме того, узел System содержит подузлы Disk Quotas (Дисковые квоты), Domain Name System (DNS) Client (DNS-клиент) и Windows File Protection (Защита файлов Windows).

При конфигурировании пользовательских параметров узел Administrative Templates также содержит дополнительные параметры групповой политики, хранимые в реестре, включая подузлы Start Menu & Taskbar (Панель задач и меню «Пуск»), Desktop (Рабочий стол) и Control Panel (Панель управления).

В узле Administrative Templates более 450 параметров предназначены ддя конфигурирования среды пользователя. Конфигурационные параметры компьютера сохраняются в разделе реестра HKEY_LOCAL_MA-CH1NE (HKLM), а пользовательские - в разделе HKEY_CURRENT_ USER(HKCU).

Влияние групповой политики на загрузку компьютера и регистрацию пользователя в системе

1. Восстанавливаются сетевые подключения. Загружаются службы Remote Procedure Call System Service (RPCSS) и Multiple Universal Naming Convention Provider (MUP).

2. Для компьютера загружается упорядоченный список ОГП, содержимое которого зависит от следующих факторов:

- состоит ли компьютер в домене Windows 2000 и распространяется ли на него действие групповой политики через службу Active Directory;
- от местоположения компьютера в службе каталогов Active Directory;
- если список ОГП не изменился, он не обрабатывается. Для изменения этого поведения настройте соответствующим образом параметры групповой политики.

3. Обрабатываются конфигурационные параметры компьютера. По-умолчанию это выполняется синхронно и в следующем порядке:

локальный ОГП, ОГП сайта, ОГП домена, ОГП подразделения и т. д. До завершения обработки интерфейс пользователя не отображается.

4. Выполняются сценарии загрузки. По умолчанию это происходит в скрытом режиме и синхронно; перед выполнением следующего сценария должен завершиться текущий сценарий, или должен наступить тайм-аут для текущего сценария.

5 Пользователь нажимает Ctrl+Alt+Del для входа в систему.

6 После проверки имени и пароля загружается профиль пользователя, на который распространяются параметры локальной групповой политики.

7 Для пользователя загружается упорядоченный список ОГП, содержимое которого зависит от следующих факторов:

- является ли пользователь членом домена Windows 2000 и распространяется ли на него действие групповой политики через службы Active Directory;
- включено ли замыкание на себя, а также в каком режиме (Merge или Replace).
- от местоположения пользователя в службе каталогов Active Directory;
- если список ОГП не изменился, он не обрабатывается. Для изменения этой ситуации настройте соответствующим образом параметры групповой политики.

8. Обрабатываются пользовательские параметры. По умолчанию это выполняется синхронно и в следующем порядке: локальный ОГП, ОГП сайта, ОГП домена, ОГП подразделения и т. д. До завершения обработки интерфейс пользователя не отображается.

9. Выполняются сценарии входа в систему. Сценарии входа, основанные на групповой политике, по умолчанию выполняются в скрытом режиме и асинхронно. Сценарий объекта пользователя выполняется последним.

10. Отображается пользовательский интерфейс ОС, соответствующий групповой политике.

Порядок обработки групповой политики

Настройки групповой политики обрабатываются в порядке, описанном ниже.

1Локальный ОГП — на каждом компьютере с Windows 2000 имеется один ОГП, хранящийся локально.

2ОГП сайта — следующими обрабатываются любые ОГП, настроенные для сайта. Обработка осуществляется синхронно; порядок обработки определяется администратором.

3ОГП домена — обработка всех ОГП, настроенных для домена, осуществляется синхронно; порядок обработки определяется администратором.

4ОГП организационной единицы — первыми обрабатываются ОГП связанные с ОП, расположенными выше всех в иерархии Active Directory. Затем обрабатываются ОГП ОП более низкого уровня и т. д. Последними обрабатываются ОГП, связанные с ОП, куда входят пользователи или компьютеры.

Исключения в порядке обработки по умолчанию

- Компьютер, состоящий в рабочей группе, обрабатывает только локальный ОГП.
- No Override (Не перекрывать). Для любого ОГП, связанного с сайтом, доменом или подразделением (но не локальным ОГП), разрешается задать параметр No Override по отношению к сайту, домену или подразделению так, что, ни один из параметров политики не будет перезаписан. При назначении более чем одному ОГП параметра No Override приоритет имеет наивысший в иерархии Active Directory параметр (или наивысший в иерархии, заданной администратором на каждом определенном уровне в Active Directory).
- Block Policy Inheritance (Блокировать наследование политики). Для наследования групповой политики любого сайта, домена или подразделения достаточно выборочно пометить флажок Block Policy Inheritance. Впрочем, параметры ОГП, для которых задан параметр No Override, применяются всегда, их нельзя блокировать. Параметр Block Policy Inheritance применяется непосредственно к сайту, домену или подразделению. Он неприменим ни к ОГП, ни к ссылкам на ОГП. Таким образом, Block Policy Inheritance предотвращает все попытки распространения параметров

групповой политики на сайт, домен или подразделение от высшего иерархического уровня (по ссылке на родительский объект в иерархии Active Directory), вне зависимости от того, где в иерархии были заданы эти параметры.

· Loopback (Замыкание на себя) — дополнительный параметр групповой политики, который необходим на компьютерах в среде, требующей нестандартной организации управления. Замыкание на себя — альтернативный способ получения упорядоченного списка ОГП, параметры пользовательской конфигурации которых влияют на среду пользователя. По умолчанию пользовательские параметры берутся из списка ОГП, зависящего от расположения объекта пользователя в иерархии Active Directory. Параметр замыкания на себя, как и любой другой параметр политики, может иметь одно из трех состояний: Not Configured (На задана), Enabled (Включена) или Disabled (Отключена). В состоянии Enabled действуют параметры Merge (Слияние) или Replace (Замена).

• Замыкание на себя с заменой. В этом случае список ОГП для данного пользователя полностью заменяется списком ОГП полученным для компьютера при его загрузке. ОГП компьютера заменяют пользовательские ОГП, которые обычно применяются к данному пользователю.

• Замыкание на себя со слиянием. В этом случае список ОГП объединяется. Список ОГП, полученный для компьютера при его загрузке (см. пункт 2 в разделе «Влияние групповой политики на загрузку компьютера и регистрацию пользователя в системе») добавляется к списку ОГП, полученному для пользователя при его регистрации (пункт 7). Список ОГП для компьютера применяется позже и поэтому при возникновении конфликтов с параметрами, указанными в пользовательском списке, имеет приоритет.

Наследование групповой политики

В общем, групповая политика передается от родительских к дочерним контейнерам. Если определенная групповая политика назначена на верхнем уровне родительского контейнера, то она применяется для всех контейнеров ниже родительского, включая объекты пользователей и компьютеров в каждом контейнере. Однако при применении определенной групповой политики к дочернему контейнеру эта политика будет более приоритетной, чем наследуемая от родительского контейнера.

Ненастроенные параметры политики для родительского подразделения не наследуются дочерним подразделением. Отключенные параметры политики наследуются как отключенные. Если политика настроена для родительского подразделения, но не настроена для дочернего, то дочернее подразделение наследует ее от родительского.

Если родительская и дочерняя политики совместимы, то помимо параметров родительской политики применяются и параметры дочерней. Политики наследуются до тех пор, пока они совместимы. Например, если родительская политика помещает определенную папку на рабочий стол, а дочерняя политика помещает на рабочий стол еще одну папку, то пользователь увидит обе папки.

Конфигурация безопасности

Расширение Security Settings (Параметры безопасности) оснастки Group Policy (Групповая политика) применяется для настройки конфигурации безопасности компьютеров и групп. На этом занятии усматриваются параметры конфигурации безопасности.

Параметры конфигурации безопасности

Конфигурация безопасности (security configuration) содержит параметры для всех областей безопасности (security area) Windows 2000. В расширении Security Settings оснастки Group Policy можно настроить параметры безопасности для нелокальных ОГП из следующих узлов:

• Account policies (Политики учетных записей);
• Local policies (Локальные политики);
• Event log (Журнал событий);
• Restricted groups (Группы с ограниченным доступом);
• System services (Системные службы);
• Registry (Реестр);
• File system (Файловая система);
• Public key policies (Политики открытого ключа);

' IP security policies (Политики безопасности IP).

Узел Account Policies

Политики из этого узла распространяются на учетные записи пользователей. К атрибутам этого узла относятся:

· Password Policy (Политика паролей) — определяет параметры парольной защиты для доменных или локальных учетных записей, например обязательный ввод пароля или срок его действия;

· Account Lockout Policy (Политика блокировки учетной записи) — определяет, когда и какие доменные или локальные учетные записи будут заблокированы;

· Kerberos Policy (Политика Kerberos) — определяет параметры протокола Kerberos для доменных учетных записей, например срок жизни билета или принудительные ограничения на вход пользователей.

Узел Local Policies

Содержит параметры безопасности компьютера, на котором работает приложение или пользователь. Локальные политики определяются компьютером, на котором регистрируется пользователь, и разрешениями, которые ему предоставлены на данном компьютере. Данная область безопасности содержит следующие атрибуты:

• Audit Policy (Политика аудита) — определяет события, которые регистрируются в журнале безопасности (успешные, неудачные и теи другие). Журнал безопасности является частью оснастки EventViewer (Просмотр событий);

• User Rights Assignment (Назначение прав пользователя) — определяет, какие пользователи и группы обладают правами на вход в систему и выполнение задач;

• Security Options (Параметры безопасности) — включают или отключают такие параметры безопасности для компьютера, как цифровая подпись данных, имена учетных записей Administrator (Администратор) и Guest (Гость), доступ к флоппи-дисководам и при

водам CD-ROM, установка драйверов и приглашения на вход в систему.

Локальные политики, по определению, применяются к локальному компьютеру. Локальные параметры, импортированные в ОГП Active Directory, влияют на локальные параметры безопасности каждого компьютера, к которому применяется данный ОГП.

Узел Event Log

В этой области безопасности определяются атрибуты, относящиеся К журналам Application (Журнал приложений), Security (Журнал безопасности) и System (Журнал системы): максимальный размер, права доступа к каждому журналу, а также способы их хранения.

Узел Restricted Groups

Данная возможность является новым важным средством безопасности, распространяющимся на членов группы. Группы с ограниченным доступом автоматически обеспечивают безопасность на основе членства в стандартных группах Windows 2000, таких, как Administrators (Администраторы), Power Users (Опытные пользователи), Print Operators (Операторы печати), Server Operators (Операторы сервера) и Domain Admins (Администраторы домена), автоматически включены в состав Restricted Groups. Позже в список безопасности групп с ограниченным доступом можно добавить другие требуемые группы или Разрешения.

узел Public Key Policies

Эта область безопасности предназначена для настройки агентов восстановления шифрованных данных, доменных корней и доверенных центров сертификации.

Узел IP Security Policies

Эта область безопасности предназначена для настройки безопасного обмена данными в IP-сетях.

Аудит

Под аудитом (auditing) в Windows 2000 подразумевается процесс контроля действий пользователей и операционной системы, которые называются событиями (events). Посредством аудита определяются события, которые необходимо записать в журнал безопасности, например попытки

законного и незаконного входа в систему, события, связанные с созданием, открытием или удалением файлов, и др. Каждая запись в журнале безопасности содержит следующую информацию:

• описание действия;

• имя пользователя, который его совершил;

• время и результат (успех или неудача) события.

Использование политики аудита

Политика аудита (audit policy) определяет категории событий, которые записываются в журнал безопасности каждого компьютера. Журнал безопасности позволяет регистрировать любые события, которые вы укажете.

Событие записывается в журнал безопасности того компьютера, где оно произошло. Например, неудачная попытка войти в компьютер домена фиксируется в журнале безопасности контроллера домена, так как именно он не смог удостовериться в личности пользователя-Политика аудита позволяет:

• выявить успешные и неудачные события, например попытки войти в систему, доступ к определенным файлам, изменение учетных записей пользователей, членство групп и другие параметры безопасности;

• устранить или минимизировать риск непредусмотренного использования ресурсов.

Рекомендации по настройке политики аудита

при планировании политики аудита необходимо определить компьютеры, подлежащие аудиту, и события, которые требуется на них регистрировать. По умолчанию аудит выключен.

После определения подлежащих аудиту событий необходимо выбрать, какие события стоит регистрировать: успешные, неудачные или и те, и другие. Регистрация успешных событий покажет, как часто пользователи и операционная система обращаются к файлам, принтерам и другим объектам. Эта информация пригодится при планировании использования ресурсов. Регистрация неудачных событий выявит нарушения безопасности. Например, при обнаружении нескольких неудачных попыток доступа, особенно в нерабочее время, можно сделать вывод, что кто-то пытается проникнуть в систему.

Правила, которыми следует руководствоваться при настройке политики аудита:

• Определите, собираетесь ли вы контролировать тенденции использования системы. В этом случае надо архивировать журналы событий. Это позволит проследить изменение использования системных ресурсов во времени и нарастить их до того, как выявится их нехватка.

• Регулярно просматривайте журнал безопасности. Для этого составьте расписание и следуйте ему. Ведь одного аудита недостаточно Для обнаружения нарушений режима безопасности.

• Политика аудита должна быть полезна и управляема. Всегда выполняйте аудит уязвимых и конфиденциальных данных. Регистрируйте только те события, которые содержат существенную информацию.

• Настройте аудит доступа к ресурсам для группы Everyone, а не для группы Users. Таким образом, вы проведете аудит доступа, всех, кто подключается по сети, а не только пользователей, для которых созданы учетные записи. Настройте также аудит неудачных попыток доступа для группы Everyone.

• Настройте аудит всех действий администраторов. Это позволит выявить все дополнения или изменения, сделанные администратором.

События, аудит которых рекомендован

Событие, подлежащее аудиту - Потенциальная угроза

Неудачные попытки входа/выхода из системы - Взлом путем подбора пароля

Успешные попытки входа/выхода из системы - Взлом с помощью украденного пароля

Применение пользователем своих прав, управление пользователями и группами, изменение политики безопасности, включение и выключение компьютера, системные события - Злоупотребление привилегиями

События, связанные с доступом - доступ к файлам и другим объектам

Аудит доступа на чтение или запись секретных файлов из Диспетчера файлов подозрительными пользователями или группами - Несанкционированный доступ к файлам

Аудит успешного и неуспешного доступа к файловым принтерам а также аудит событий доступа к объектам. Аудит доступа к принтерам через Диспетчер печати подозрительными пользователями или группами - Несанкционированный доступ

События, связанные с записью программных файлов (.exe или dll). События, генерируемые процессами. Запуск определенных программ. Попытки изменения программных файлов и создания непредусмотренных процессов - Заражение данных вирусом

**Администрирование БД**

Администратор базы данных — это должностное лицо, которое отвечает за обслуживание СУБД.

АБД имеет много различных обязанностей, но главное для него — обеспечить постоянную работу сервера и предоставить пользователям доступ к нужной информации в любое время. Кроме того, АБД должен делать все от него зависящее, чтобы обеспечить защиту данных и свести к минимуму вероятность их потери.

Кто может стать АБД

Администратором базы данных может стать человек, который занимается разработкой базы данных и управлением ею. Это может быть программист, который принял на себя ответственность за обслуживание SQL Server на время разработки проекта и настолько увлекся этим занятием, что изменил профиль своей работы. Это может быть и системный администратор, которому вменили в обязанности также поддержку SQL Server. Это может быть даже переквалифицировавшийся специалист из другой области, например бухгалтер. Если вы тоже хотите стать АБД, вам необходимо следующее:

- хорошее знание операционных систем Microsoft Windows;
- знание языка структурированных запросов (SQL);
- умение разрабатывать базы данных;
- общее понятие о сетевых архитектурах (например, клиент/сервер, Internet/intranet, Enterprise);
- знание Microsoft SQL Server.

Совет специалиста микрософт:

Если вы являетесь членом команды техобслуживания, которой требуется администратор Microsoft SQL Server, вот вам мой совет: вызовитесь на эту должность. Во-первых, это прекрасная работа. Во-вторых, хорошие АБД нужны всегда и везде. И в-третьих, обычно им платят больше, чем разработчикам.

Обязанности АБД

1.Установка и модернизация SQL Server

Администратор баз данных отвечает за установку и модернизацию существующей версии SQL Server. Если модернизируется SQL Server, то АБД отвечает за то, чтобы в случае неудачи можно было вернуться к прежней версии SQL Server и использовать ее, пока все проблемы не будут решены. АБД отвечает также за применение пакетов обновления SQL Server. Пакет обновления (service pack) — это не модернизация, а только установка текущей версии программного обеспечения, в которой исправлены разнообразные ошибки, найденные после выпуска продукта.

2.Наблюдение за состоянием сервера базы данных и его соответствующая настройка

Наблюдение за состоянием сервера базы данных необходимо для того, чтобы убедиться в следующем:

- сервер работает с оптимальной производительностью;
- в журнале ошибок или журнале событий не зафиксированы ошибки в работе СУБД;
- обслуживание баз данных проводится повседневно, а всей системы в целом — периодически (последнее входит в обязанности системного администратора).

**3.Правильное использование памяти**

SQL Server 2000 позволяет автоматически увеличивать размеры баз данных и журналов транзакций, но вы можете установить для них фиксированные размеры. В любом случае правильное использование памяти означает, что вы должны знать, сколько памяти требуется, и по мере необходимости добавлять новые дисковые накопители (жесткие диски).

Резервное копирование и восстановление данных

Резервное копирование и восстановление данных — самые важные задачи АБД. Сюда входит следующее:

- разработка стандартов и графика резервного копирования;
- разработка процедур восстановления для каждой базы данных;
- проверка соответствия графика резервного копирования требованиям к восстановлению данных.

Управление пользователями базы данных и обеспечение безопасности

В SQL Server 2000 АБД тесно сотрудничает с администратором Windows NT/2000 в области присвоения пользователям прав доступа к базе данных. Когда дело не касается сферы влияния Windows NT/2000, АБД разрешает пользователям такой доступ сам. Он отвечает также за назначение пользователю той или иной базы данных и определение его прав доступа. В зависимости от этих прав, пользователь может (или не может) обращаться к различным объектам базы данных, например к таблицам, представлениям и хранимым процедурам.

Сотрудничество с разработчиками

Для АБД очень важно тесно сотрудничать с командой разработчиков в области общего проектирования базы данных. Сюда относится создание нормализованных баз данных, настройка, назначение правильных индексов, а также разработка триггеров и хранимых процедур. В среде SQL Server 2000 хороший АБД сможет подсказать разработчикам, как использовать преимущества мастера настройки индексов SQL Server (SQL Server Index Tuning Wizard) и профилировщика SQL Server (SQL Server Profiler).

Определение соглашений и стандартов

Администратор баз данных должен установить для SQL Server и баз данных соглашения по наименованию и стандарты, а также следить за тем, чтобы все пользователи их придерживались.

Перенос данных

Администратор баз данных отвечает за импорт и экспорт данных в SQL Server и из него. В настоящее время наметилась тенденция к уменьшению размеров систем клиент/сервер и их сочетанию с мэйнфреймами и Web-технологиями для создания систем управления предприятием (типа Enterprise). В таких условиях импорт данных из мэйнфрейма в SQL Server стал обычным делом; еще больше эта практика распространилась в связи с появлением служб преобразования данных (Data Transformation Services — DTS) SQL Server 2000. Хорошие администраторы, знающие DTS, в ближайшее время будут в большой цене, так как сейчас фирмы стремятся преобразовать устаревшие системы в системы типа Enterprise.

Репликация данных

В версии SQL Server 2000 появились новые возможности репликации, например репликация путем слияния (двусторонняя изолированная репликация). Управление репликацией и настройка ее топологий станет очень важной задачей АБД, так как репликация — это потрясающая возможность, которая будет играть важную роль в работе многих организаций.

Хранилище данных

В SQL Server 2000 добавились новые возможности складирования данных, для использования которых АБД придется изучить дополнительный продукт (Microsoft OLAP Server) и его архитектуру. С появлением этой возможности перед АБД встают новые интересные задачи!

Составление графика обработки событий

Администратор базы данных отвечает за составление графика обработки различных событий с помощью стандартных средств Windows NT/2000 и SQL Server. Это поможет успешно справляться с различными задачами, такими как создание резервных копий и процессов репликации.

Обеспечение круглосуточного доступа к данным

Сервер базы данных должен работать круглосуточно, обеспечивая доступ к базам данных. Будьте готовы через некоторое время выполнить необходимые операции по поддержке работоспособности СУБД и ее модернизации. Постарайтесь также выдержать этот ужасный сигнал пейджера. Если сервер базы данных "сляжет", вам придется "поднять" его и заставить работать. В конце концов, это ваша работа.

Как АБД взаимодействует с другими членами команды

АБД должен взаимодействовать с системным и сетевым администраторами, разработчиками и пользователями. Вообще говоря, эти взаимоотношения трудно определить однозначно, так как в каждой организации есть люди, занимающие сразу несколько должностей.

Системный и сетевой администраторы

Взаимодействие АБД с сетевым администратором касается, прежде всего, типов используемых сетевых протоколов и сетевого адреса или номера порта, который можно выбрать для сервера. Если пользователи жалуются на медленное выполнение запросов, в то время как SQL Server выполняет запросы очень быстро, то АБД вместе с сетевым администратором должны попытаться найти причину этих проблем, связанную с сетью.

Как правило, АБД более тесно взаимодействует с системным администратором, чем с сетевым. Системный администратор отвечает за настройку сервера Windows NT /2000, на котором работает SQL Server. В его обязанности входит также добавление накопителей на жестких дисках и выделение памяти, необходимой для размещения баз данных. Если вы собираетесь использовать интегрированную с SQL Server систему доступа пользователей, то должны вместе с системным администратором корректно определить учетные записи для пользователей и групп пользователей в Windows NT/2000. Различные типы процедур резервного копирования и восстановления данных для Windows NT/2000 Server и SQL Server должны быть проработаны обеими сторонами, так как системному администратору может понадобиться восстановить системный диск, на котором содержится база данных или ее резервная копия.

Разработчики

Различия между организациями больше всего отражаются на взаимодействии АБД с разработчиками. В одних организациях такое взаимодействие очень тесное, а в других — практически отсутствует; во втором случае АБД только безмолвно принимает все, что сделали разработчики, не делая никаких замечаний и не давая рекомендаций. Конечно, для получения оптимального результата АБД должен как можно более тес,но сотрудничать с разработчиками. В конце концов, именно он будет обслуживать базу данных и в большинстве случаев у него больше опыта разработки и настройки реляционных баз данных. Поэтому АБД должен принимать активное участие в разработке, давать советы, помогать и быть в курсе всех событий. Его помощь должна выражаться в правильном выборе индексов, оптимизации запросов и хранимых процедур, а также в предоставлении разработчикам необходимой информации.

Пользователи

В большинстве организаций взаимодействие АБД с пользователями ограничивается поддержкой их учетных записей, определением прав доступа и восстановлением баз данных.

SQL Server — это обладающая высокой производительностью СУБД, которая глубоко интегрирована с операционными системами Windows NT/2000 и Windows 9x/Me, благодаря чему SQL Server может пользоваться всеми преимуществами функций, обеспечиваемыми этими операционными системами. SQL Server — мощная СУБД, в полной мере отвечающая потребностям современных сложных систем типа клиент/сервер.

Архитектура

Благодаря глубокой интеграции SQL Server с операционной системой, под управлением которой она работает, в вашем распоряжении имеются следующие важные возможности:

- симметричная мультипроцессорная обработка (Symmetric multiprocessing — SMP);
- переносимость – работа на многих ОС;
- сетевая независимость;
- надежность.

Симметричная мультипроцессорная обработка (SMP)

Использование SMP позволяет SQL Server повысить производительность с помощью дополнительных процессоров. SQL Server 2000 Enterprise Edition под управлением Windows 2000 Datacenter поддерживает до 32 процессоров и до 64 Гбайт оперативной памяти. SQL Server может автоматически запустить запрос для параллельного выполнения на двух или более процессорах.

Все это происходит без вмешательства со стороны пользователя; администраторы также освобождаются от проблем с управлением несколькими процессорами.

В версии SQL Server для Windows 9x поддержка SMP не реализована.

Сетевая независимость

Операционные системы Windows NT/2000 и Windows 9x/Me поддерживают несколько различных типов сетевых протоколов. Этот уровень поддержки простирается вплоть до подключения клиентской части SQL Server. Таким образом, вы можете выбрать сетевой протокол, который будет наиболее полно отвечать вашим потребностям. В настоящее время поддерживаются следующие сетевые протоколы: TCP/IP, IPX/SPX, Named Pipes, AppleTalk и Banyan Vines.

Надежность

Windows NT/2000 и SQL Server обеспечивают надежную защиту данных от непредвиденного сбоя или отказа системы, динамическое управление памятью, предварительное составление графика выполнения задач и удаленное управление. Эти возможности позволяют поддерживать SQL Server в рабочем состоянии 24 часа в сутки и 7 дней в неделю.

Разработка стратегии и плана инсталляции

Разработка плана инсталляции начинается с анализа требований, вытекающих из характера деятельности предприятия, и пожеланий пользователей. Вы должны рассмотреть широкий круг вопросов, начиная с выбора и приобретения аппаратного обеспечения и заканчивая принятием решений по установке конкретных параметров SQL Server. Начните с рассмотрения системных требования и пожеланий пользователей. На основании этого изучите возможные конфигурации аппаратного обеспечения и параметры SQL Server. Затем составьте список параметров, чтобы пользоваться им во время инсталляции, и, наконец, установите SQL Server.

Этап 1. Определение системных требований и пожеланий пользователей

Как определить системные требования и узнать пожелания пользователей? Очень просто: задавайте вопросы и анализируйте ответы. Начните с пожеланий пользователей и требований, вытекающих из характера деятельности предприятия, и вы сможете решить, какое аппаратное обеспечение вам необходимо. Итак, для начала найдите ответы на следующие вопросы:

- Каково назначение системы?
- Какие требования предъявляются к СУБД?
- Каковы пожелания пользователей и какие требования вытекают из характера деятельности предприятия?
- Сколько это будет стоить?

Каково назначение системы

Первый вопрос, который вы должны себе задать: для чего предназначена система и сколько пользователей будут одновременно ее применять (например, система создается для одного отдела, состоящего из 10 пользователей, или для большого предприятия, на котором работают тысячи пользователей). Чем больше пользователей поддерживает система, тем выше требования к быстродействию, оперативной памяти и объему жестких дисков сервера. Компьютер предназначен исключительно для запуска SQL Server или он будет выполнять еще какие-либо функции (например, печать файлов)? Заменяет ли новая система старую в результате модернизации или изменения размера базы данных? Если это действительно замена старой системы, то у вас будет довольно много необходимой информации (например, текущая нагрузка системы и ее недостатки). Система является действующей или тестовой, находящейся на стадии разработки? Для действующего сервера необходимы более мощная защита от сбоев и более объемные жесткие диски, чем для сервера тестовой системы.

Каковы требования базы данных

Какие требования предъявляет к серверу база данных? Что SQL Server будет поддерживать в первую очередь: системы-принятия решения или системы выполнения транзакций? Насколько велика будет предполагаемая нагрузка при выполнении транзакций? Если система предназначена для выполнения транзакции, попробуйте определить предполагаемое количество транзакций в день и способ их обработки. Например, сервер может восемь часов простаивать, а затем в течение нескольких часов обрабатывать все транзакции либо равномерно обрабатывать транзакции целый

день. Каков ожидаемый размер базы данных? Возможно, вы перемещаете базы данных из старой системы на SQL Server в результате модернизации или изменения их размера. Если это так, вы можете получить информацию о текущем и ожидаемом размерах базы данных и о текущей нагрузке транзакций на систему.

Каковы требования и нужды пользователей

Всегда очень важно понять, чего требуют и чего ожидают пользователи SQL Server. На какое время ответа со стороны системы рассчитывают пользователи? Сколько пользователей будет подключено к SQL Server одновременно? Какие требования к резервному копированию и объему памяти вытекают из характера деятельности предприятия? Какие требования к резервному копированию и объему памяти предъявляют пользователи? Когда вы узнаете нужды пользователей, постарайтесь определить, сможете ли вы создать систему, отвечающую этим нуждам. Возможно, вам придется опустить их с небес на землю, чтобы они осознали реальные возможности системы.

Сколько это будет стоить

Наверное, этот вопрос нужно ставить первым! В реальной жизни разница между той системой, которую вы хотите, и той, которую получаете, обусловлена только количеством средств, имеющихся в вашем распоряжении. Но можно утешиться тем, то цены на компьютеры постоянно снижаются и стоимость нужного вам сервера становится все более приемлемой.

Этап 2. Выбор платформы

Получив ответы на вопросы первого этапа, вы будете готовы к выбору платформы аппаратного обеспечения для SQL Server. Чтобы выбрать платформу, необходимо определиться по следующим четырем пунктам:

- аппаратное обеспечение (включая количество процессоров и необходимые периферийные устройства);
- объем оперативной памяти;
- емкость накопителей на жестких дисках;
- тип файловой системы.

Аппаратное обеспечение

При выборе платформы аппаратного обеспечения вы должны проверить, есть ли в списке совместимости аппаратного обеспечения для Windows NT/2000 марка и модель компьютера, который вы хотите использовать в качестве сервера. Приобретая компьютер, обязательно сообщите фирме-продавцу, что вы собираетесь использовать его в качестве сервера базы данных.

СОВЕТ Микрософт

Вы убережете себя от многих проблем, если будете использовать только те компьютеры, которые сертифицированы корпорацией Microsoft для работы с операционной системой Windows NT/2000.

Нужен ли мне компьютер с несколькими процессорами?

Система Windows NT способна поддерживать до четырех процессоров, а Windows 2000 — восемь. SQL Server может воспользоваться преимуществами такой многопроцессорной поддержки без каких-либо специальных дополнительных модулей или изменений конфигурации.

Оперативная память

Для SQL Server необходимо как минимум 32 Мбайт оперативной памяти для версий Personal и Desktop, и 64 Мбайт — для всех остальных версий В новой версии SQL Server вам больше не нужно вручную распределять оперативную память и указывать способ ее использования. SQL Server 2000 динамически регулирует используемый объем памяти в зависимости от текущих требований и состояния операционной системы компьютера, на котором он работает.

Независимо от начального объема памяти, спустя некоторое время вы сможете более точно определить, сколько памяти необходимо SQL Server для работы.

Накопители на жестких дисках

Вы должны принять еще одно важное решение: выбрать тип накопителей на жестких дисках и контроллеров к ним. Правильный выбор жестких дисков окажет существенное влияние на общую производительность SQL Server и на отказоустойчивость системы в целом.

Уделите особое внимание выбору типа накопителей на жестких дисках. Выполнение операций ввода-вывода — одно из узких мест всех СУБД

Такое же значение, как скорость жестких дисков, имеет и отказоустойчивость современных дисковых накопителей. Следует максимально защитить базу данных, обеспечив при этом оптимальную производительность. Один из возможных вариантов — использовать RAID-массивы (Redundant Array of Inexpensive Disks — избыточный массив недорогих дисков). В конфигурации RAID используется несколько дисков, составляющих одно логическое разделяемое устройство. Таким образом, логически RAID-массив представляет собой одно устройство, а физически это несколько жестких дисков, работающих под управлением соответствующего программного и аппаратного обеспечения. В RAID-конфигурациях файлы можно распределять по нескольким физическим устройствам, что позволяет достичь высокой производительности. Другим преимуществом RAID-массивов является их отказоустойчивость и способность к восстановлению данных. RAID-массив 5то уровня позволяет в случае отказа одного диска полностью восстановить содержащиеся на нем данные. При добавлении нового диска RAID-массив автоматически восстановит данные, которые были на потерянном устройстве, и поместит их на новый диск. RAID-массив 5-го уровня обеспечивает высокую степень защиты и оптимальную производительность базы данных. RAID-массивы можно создавать на основе аппаратного или программного обеспечения для системы Windows NT/2000. Как правило, RAID-массивы на основе аппаратного обеспечения более быстродействующие, чем массивы, построенные на основе программного обеспечения.

Файловая система

Какую файловую систему следует использовать, работая с Windows NT/2000,— NTFS (New Technology File System — система новой файловой технологии) или FAT (File Allocation Table— таблица размещения файлов)? Что касается производительности, то это не имеет никакого значения, поскольку разница в производительности для двух этих файловых систем совершенно незначительна. В целом NTFS быстрее выполняет операции чтения, а FAT — операции записи. Однако, применяя NTFS, вы можете воспользоваться преимуществами системы безопасности Windows NT/2000.

Выбор платформы

Правильно выбранная платформа для SQL Server — это сервер, имеющий максимально возможную конфигурацию из тех, которые вы можете себе позволить, и обеспечивающий нормальную работу SQL Server! Хорошая конфигурация для SQL Server: компьютер с одним или несколькими процессорами, имеющий минимум 256 Мбайт оперативной памяти. Используйте для размещения баз данных RAID-массив 5-го уровня. Поместите журналы транзакций на RAID-массив 1-го уровня (с зеркальными дисками) с разделением данных, а операционную систему и SQL Server — на обычное дисковое устройство или RAID-массив 1-го уровня.

Этап 3. Важные вопросы, требующие ответа

Вам нужно твердо знать ответы на ряд вопросов.

- Куда поместить файлы баз данных?
- Как назвать экземпляр сервера?
- Каков порядок сортировки и кодировки символов?
- Какой сетевой протокол использовать?
- Под какой учетной записью Windows NT/2000 нужно запускать службы SQL Server и SQL Server Agent?

Расположение файлов баз данных

Во время инсталляции вам нужно будет ответить, где следует установить системные базы данных SQL Server (т.е. указать устройство и путь). К системным базам данных от носятся следующие:

- master — база данных конфигурации SQL Server;
- mode1 — база, которая служит в качестве шаблона для создания других баз данных;
- tempdb — область временного хранения данных (временная база данных);
- msdb — база данных для хранения графика работ и база данных SQL Serve: Agent;
- Northwind и Pubs — примеры баз данных.

Стандартное место расположения файлов данных— подкаталог \Data корневого ка талога SQL Server. При инсталляции вы можете выбрать другое место расположена файлов или оставить стандартную установку. Выберите устройство, на котором достаточно места для дальнейшего расширения файлов баз данных.

Базы данных master msdb и model обычно увеличиваются не очень быстро (к ним добавляется всего не сколько мегабайтов в неделю). Но база данных tempdb— это совсем другое дело. SQL Server 2000 при необходимости автоматически увеличивает базу данных tempdb, если превышается ее предельный размер, заданный во время инсталляции. А когда SQL Server останавливают или перезапускают, tempdb автоматически возвращается к первоначальному размеру. Поэтому имеет смысл выбрать для базы данных tempdb устройство или RAID-массив, где достаточно места для ее расширения; это устройство должно также обеспечивать высокую производительность.

Имя экземпляра

SQL Server 2000 позволяет установить несколько экземпляров ядра базы данных SQL Server. Если устанавливается один экземпляр SQL Server, то по умолчанию его именем является имя компьютера. Если устанавливается много экземпляров, то каждому из них необходимо присвоить уникальное имя. Имена экземпляров не чувствительны к регистру, их длина не может превышать 16 символов. Первым символом имени должна быть буква, символ подчеркивания, символ номера или амперсант.

Параметры сортировки и кодировки символов

SQL Server 2000 не требует отдельного задания способов сортировки и набора символов для обычных данных и для символов Unicode. Выбор типа сортировки (идентифицируемый именем) задает правила упорядочения и сравнения как для обычных данных, так и для символов Unicode. Например, можно задать сравнение, нечувствительное к регистру символов, или сравнение двоичных эквивалентов символов. В параметры сортировки входят наборы символов, используемых данными. Символы Unicode имеют вдвое больший размер, чем символы ANSI. В ANSI используется 256 символов, а в Unicode — 65 356 символов. При установке SQL Server используются параметры сортировки и кодировки установленной операционной системы Windows и по умолчанию сервер самостоятельно настраивает все эти параметры. Рекомендуется придерживаться этой установки по умолчанию.

Сетевые протоколы

Поскольку SQL Server может одновременно поддерживать несколько различных сетевых протоколов, то клиенты, использующие TCP/IP, могут подключаться к SQL Server одновременно с клиентами, использующими IPX/SPX. Во время инсталляции SQL Server устанавливаются различные сетевые библиотеки, предназначенные для обмена сетевыми сообщениями с другими серверами и клиентскими рабочими станциями. При инсталляции SQL Server 2000 по умолчанию устанавливается поддержка нескольких сетевых протоколов.

Существует 2 режима безопастности:

• Режим аутентификации Windows NT. Использует преимущества системы безопасности Windows NT/2000, в которой задействуется механизм создания учетных записей на сервере NT. Данный режим требует установки доверительного соединения с сервером (trusted connection) и может быть реализован через протокол Named Pipes (именованный канал) или мультипротокол.

• Смешанный режим. Позволяет пользователям подключиться к SQL Server с помощью режимов аутентификации Windows NT и SQL Server. В последнем случае пользователь, подключающийся к SQL Server, сообщает имя и пароль, который проверяется SQL Server по системной таблице. Пользователи, применяющие доверительные соединения, могут подключиться к SQL Server с помощью режима аутентификации Windows NT.

Протокол Named Pipes

Это стандартный протокол, устанавливаемый SQL Server. Он обеспечивает обмен сообщениями между процессами, происходящими на локальном сервере или на серверах в сети, и используется в сетях Windows NT.

Мультипротокол

Мультипротокол использует для передачи сообщений механизм вызова удаленной процедуры (Remote Procedure Call — RPC) Windows NT и не требует никакой дополнительной настройки. В настоящее время мультипротокол поддерживает протоколы NWLink IPX/SPX, TCP/IP и Named Pipes. Он позволяет пользователям протоколов IPX/SPX и TCP/IP применять преимущества аутентификации пользователей Windows NT.

Протокол NWLink IPX/SPX

Это известный сетевой протокол для сетей Novell. Если во время инсталляции SQL Server вы выберете именно его, то вас попросят указать имя сервисной службы Novell Bindery, чтобы зарегистрировать SQL Server.

протокол TCP/IP

Это популярный протокол, использующийся в Internet. Если вы выберете TCP/IP, то вас попросят указать номер порта TCP/IP для SQL Server, который будет использоваться для соединений с клиентами. Стандартный номер порта для SQL Server — 1433.

Гарантией того, что ваша система будет работать эффективно и правильно является грамотное администрирование и регулярное выполнение задач обслуживания баз данных. SQL Server содержит множество средств для автоматического конфигурирования, такие как динамическое управление памятью, пул памяти, использование дополнительное памяти, различные параметры. С помощью многочисленных параметров системной хранимой процедуры sp_configure можно активизировать/останавливать различные свойства:

sp_configure [ [ @configname = ] 'option_name'  [ , [ @configvalue = ] 'value' ] ]

[ @configname= ] 'option_name'

Имя параметра конфигурации. Аргумент option_name имеет типvarchar(35) и значение по умолчанию NULL.

[ @configvalue= ] 'value'

Новое значение параметра конфигурации. Аргумент value имеет тип int и значение по умолчанию NULL. Максимальное значение зависит от конкретного параметра.

```
USE master;
GO
EXEC sp_configure 'recovery interval', '3';
RECONFIGURE WITH OVERRIDE;
```

Необходимым фактором, влияющим на бесперебойную работу системы, является план обслуживания, который следует тщательно настраивать и грамотно управлять. Знание системных хранимых процедур sp_createstats и sp_autostats помогут в решении повседневных задач.

SQL Server содержит множество автоматических средств, предназначенных для снижения расходов, которые обычно связаны с конфигурированием и настройкой системы управления реляционными базами данных (RDBMS).

2.1 Динамическое управление памятью

Динамическое управление памятью позволяет SQL Server динамически конфигурировать количество памяти, используемое для буферного кэша и кэша процедур, исходя из доступной памяти системы.

Средство динамического управления памятью действует путем постоянного мониторинга доступной физической памяти в системе. SQL Server увеличивает или уменьшает пул памяти SQL Server, исходя из своих потребностей и количества доступной памяти. Это может оказаться очень полезным в системах, где количество используемой памяти относительно стабильно, но если количество памяти, используемое процессами, не связанными с SQL Server, варьируется, то SQL Server будет постоянно изменять свое распределение памяти, и это может создавать проблемы.

2.2 Пул памяти

Объектный пул (англ. object pool) — порождающий шаблон проектирования, набор инициализированных и готовых к использованию объектов. Когда системе требуется объект, он не создаётся, а берётся из пула. Когда объект больше не нужен, он не уничтожается, а возвращается в пул.

Объектный пул применяется для повышения производительности, когда создание объекта в начале работы и уничтожение его в конце приводит к большим затратам. Особенно заметно повышение производительности, когда объекты часто создаются-уничтожаются, но одновременно существует лишь небольшое их число.

SQL Server динамически выделяет и освобождает память в пуле. Пул памяти содержит определенное количество памяти, которое разделяется между следующими компонентами:

- Буферный кэш. Содержит страницы базы данных, считанные в память. Буферный кэш обычно забирает основную часть пула памяти.
- Память для соединений. Используется каждым соединением с SQL Server. Память для соединений содержит структуры данных, с помощью которых отслеживается контекст каждого пользователя; это информация о позиционировании курсора, значения параметров очереди и информация хранимых процедур.
- Структуры данных. Содержит глобальную информацию о блокировках и дескрипторах базы данных, включая информацию о владельцах блокировок, о типах захваченных блокировок, а также о различных файлах и группах файлов.
- Кэш журнала. Используется для информации журнала, которая будет записана в журнал транзакций. Он также используется, когда происходит чтение последней информации, записанной в этот кэш. Использование кэша журнала повышает производительность операций записи в журналы. Кэш журнала не следует путать с буферным кэшем.
- Кэш процедур. Используется для хранения планов исполнения операторов Transact-SQL (T-SQL) и хранимых процедур, когда происходит их выполнение.

2.3 Статистика

Статистика для оптимизации запросов — это объекты, содержащие статистические сведения о распределении значений в одном или нескольких столбцах таблицы или индексированного представления.

Статистика по колонкам необходима для повышения производительности запросов в вашей системе. SQL Server может собирать статистическую информацию, касающуюся распределения значений в колонке таблицы. Оптимизатор запросов Query Optimizer затем использует эту информацию для определения оптимального плана исполнения запроса.

Статистику можно собирать по двум типам колонок:

- по тем, что являются частью индекса,
- по тем, что не входят в индекс, но используются в предикате запроса (в предложении WHERE).

Оставив принятые по умолчанию значения SQL Server для базы данных, вы разрешаете автоматическое создание обоих типов статистики в SQL Server. Статистика по индексированным колонкам создается при создании соответствующего индекса. Статистика по неиндексированным колонкам создается, когда она требуется для какого-либо запроса (только по одной колонке, а не по нескольким, как вы увидите в подразделе "Команда CREATE STATISTICS" этого раздела). Если статистика устарела (не использовалась в течение определенного периода времени), то SQL Server автоматически удаляет ее.

Вы можете создавать статистику по определенным колонкам таблицы вручную с помощью оператора T-SQL CREATE STATISTICS. Создание статистики вручную отличается от автоматического создания в том, что оно позволяет вам объединять несколько колонок, генерируя для комбинации колонок такую информацию, как среднее количество дублированных значений и отличающихся значений.

2.4 Планы обслуживания баз данных

План обслуживания – это набор задач, которые SQL Server будет автоматически выполнять по вашим базам данных согласно заданному вами расписанию. Целью плана обслуживания является автоматизация важных административных задач и снижение объема ручной работы DBA. Вы можете создавать отдельный план для каждой базы данных, несколько планов для одной базы данных или один план для нескольких баз данных.

Имеются четыре следующие основные категории административных задач, которые вы можете планировать путем создания плана обслуживания.

- Оптимизации.
- Проверки целостности.
- Резервное копирование баз данных.
- Резервное копирование журнала транзакций.

Выполнение этих задач имеет важное значение для поддержки хорошо работающей и восстанавливаемой базы данных. Типы оптимизационных задач, которые вы включите в ваш план, будут зависеть от производительности и степени использования вашей базы данных. Выполнение проверок целостности является хорошим средством, чтобы обеспечить согласованность и сохранность базы данных. А регулярное резервное копирование требуется для того, чтобы обеспечить восстанавливаемость базы данных в случае аварии системы или пользовательских ошибок. В силу особой важности операций резервного копирования вам следует разработать стратегию автоматизированного резервного копирования. Мы подробно рассмотрим каждую из этих категорий задач в данном разделе.

Для создания плана обслуживания используется мастер Database Maintenance Plan Wizard.

Вы можете выбирать следующие типы оптимизации для базы или баз данных, выбранных на предыдущем шаге.

- Reorganize data and index pages (Реорганизация страниц данных и индексов). Этот флажок указывает, что все индексы и все таблицы базы данных будут удалены и воссозданы с использованием указанного коэффициента заполнения (или количества свободного места на каждой странице), что может повысить производительность обновлений. В случае таблиц, предназначенных только для чтения, реорганизация страниц не является необходимостью. В случае таблиц, для которых часто выполняются вставки или изменения, свободное место, которое первоначально было доступно на ваших индексных страницах, постепенно заполняется, и начинает происходить фрагментация страниц.
- Update statistics used by query optimizer (Обновление статистики, используемой оптимизатором запросов) При установке этого флажка SQL Server выполнит перерасчет статистики распределения по всем индексам в соответствующей базе данных. SQL Server использует эту информацию для выбора оптимального плана исполнения для запросов.
- Remove unused space prom database files (Удалить неиспользуемое пространство из файлов базы данных) Этот флажок применяется для удаления неиспользуемого пространства; этот процесс также известен как уплотнение (сжатие) файла (file shrink). Вы можете задать, насколько большим должно стать неиспользуемое пространство, чтобы произошло сжатие файла, а также процент пространства, которое должно остаться свободным после сжатия.

Автоматизация административных задач осуществляется заданиями, оповещениями, операторами. С помощью службы SQLServerAgent можно управлять автоматизацией задач. Maintenance Plan Wizard и Create Job Wizard помогают конфигурировать задачи и планы работ. Служба SQLServerAgent имеет собственный журнал ошибок, который позволяет протоколировать любые действия, связанные со службой.

3.1 Задания

Задания – это административные задачи, которые определяются один раз и могут выполняться многократно. Вы можете запускать задание вручную, а также планировать запуск задания системой SQL Server в определенное время, в соответствии с регулярным расписанием или при возникновении оповещения. (Об оповещениях описаны далее в разделе "Оповещения".) Задания могут состоять из операторов Transact-SQL (T-SQL), команд Microsoft Windows NT или Microsoft Windows 2000, исполняемых программ или сценариев Microsoft ActiveX. Задания также автоматически создаются для вас, когда вы используете репликацию или создаете план обслуживания базы данных. Задание может состоять из одного или нескольких шагов, и каждый шаг может быть вызовом более сложного набора шагов, например обращением к хранимой процедуре. SQL Server автоматически следит за результатом выполнения заданий (успешное или неуспешное завершение); вы можете задавать оповещения, которые будут отправляться в каждом случае.

Задания могут выполняться локально на сервере, а в случае нескольких серверов в сети вы можете назначать один из серверов как главный сервер, а остальные серверы – как серверы-получатели. На главном сервере хранятся определения заданий для всех серверов, и этот сервер действует как центр обмена информацией для координирования работы всех заданий. Каждый сервер-получатель периодически подсоединяется к главному серверу, обновляет список своих заданий, если какие-либо задания изменились, загружает любые новые задания с главного сервера и затем отсоединяется для выполнения этих заданий. Когда сервер-получатель завершает какое-либо задание, он снова подсоединяется к главному серверу и сообщает о статусе его завершения.

SQL Server поддерживает журнал (историю) с информацией о выполнении задания в таблице sysjobhistory системной базы данных msdb. Вы можете просмотреть информацию журнала выполнения задания с помощью Enterprise Manager или T-SQL.

3.2 Оповещения

Оповещение – это действие, которое возникает на сервере в ответ на событие или состояние производительности. Оповещения могут реализоваться как уведомления операторам, могут инициировать запуск указанных заданий и могут перенаправлять события другому серверу. Событие – это ошибка или сообщение, которые записываются в журнал событий приложений Windows NT или Windows 2000 (вы можете просматривать этот журнал с помощью утилиты Event Viewer, поставляемой вместе с Windows NT или Windows 2000). Состояние производительности – это характеристика работы системы, доступная для мониторинга с помощью Performance Monitor (Windows NT) или System Monitor (Windows 2000), такая как процент использования ЦП или количество блокировок, используемых SQL Server. В этой лекции мы будем рассматривать System Monitor в Windows 2000, хотя Performance Monitor в Windows NT действует почти так же.

При возникновении какого-либо события служба SQLServerAgent сравнивает это событие со списком определенных вами оповещений, и если для этого события существует оповещение, то происходит запуск этого оповещения. Запуск оповещения для определенного состояния производительности происходит в том случае, если указанный объект SQL Server в System Monitor достигает определенного порогового значения производительности, например, счетчик User Connections (Количество пользовательских соединений) внутри объекта General Statistics (Общая статистика) в System Monitor. Например, вы можете указать запуск оповещения, если значение этого счетчика достигнет 50.

3.3 Операторы

Операторы – это отдельные люди, которые могут получать уведомление от SQL Server по завершении какого-либо задания или при возникновении какого-либо события. Оператор – это человек, ответственный за обслуживание одной или нескольких систем, на которых работает SQL Server. Вы уже знаете, как определять сообщение уведомления, которое будет отправляться оператору.

Имеется три метода, используемых для связи с операторами: отправка сообщений электронной почты, отправка на пейджер и использование команды NET SEND(которая отправляет сетевое сообщение на компьютер оператора.) Чтобы можно было применять каждый из этих методов, ваша система должна отвечать определенным требованиям. Для связи через электронную почту и с пейджером вы должны инсталлировать на сервере совместимый с MAPI-1 клиент ("MAPI" означает "Messaging API" – интерфейс прикладного программирования для сообщений), такой как Microsoft Outlook или Microsoft Exchange Client, и должны создать почтовый профиль для службы SQLServerAgent. Для пейджинговой связи вам нужно также инсталлировать на почтовом сервере программное обеспечение сторонних фирм для связи электронной почты с пейджером, которое обрабатывает входные сообщения электронной почты и преобразует их в пейджинговые сообщения. Чтобы использовать NET SEND, у вас должна работать операционная система Windows NT или Windows 2000, поскольку NET SEND не поддерживается в Microsoft Windows 95/98.

**Репликации**

Одним из важнейших элементов системы SQL Server является служба репликации данных.

Следует подчеркнуть, что служба репликации является составной частью стандартной версии SOL Server, поскольку поставщики других СУРБД рассматривают средства репликации как отдельный продукт, за который необходимо вносить дополнительную плату.

По сути, репликация является службой, осуществляющей гарантированное копирование информации из исходной базы данных в одну или более целевых. Средства репликации Microsoft SQL Server позволяют организовать автоматическую рассылку данных некоторого сервера на несколько других серверов с использованием ODBC (Open Database Connectivity— открытый интерфейс баз данных) или OLE DB. Используя средства ODBC или OLE DB, SQL Server 2000 обеспечивает репликацию данных в адрес получателей, не относящихся к системам SQL Server (смешанная репликация), например Microsoft Access и Oracle. Поддерживаются также анонимные подписчики в Internet. Кроме того, SQL Server 2000 позволяет непосредственно обновлять подписчиков и осуществлять репликацию методом слияния, что существенно расширяет возможности репликации.

С учетом нововведений количество возможных вариантов решений, доступных при создании приложений, становится просто ошеломляющим!

Перечислим приложения или сценарии, в которых могут применяться средства репликации SQL Server.

- Для распределения нагрузки между серверами в сети (например, для передачи произвольных запросов или отчетов на обработку серверу, отличному от исходного).
- Для перемещения определенных поднаборов данных (например, данных некоторого подразделения или данных за установленный период) с главного цен трального сервера на вспомогательные.
- При наличии в системе центральной обновляемой базы данных, когда вносимые в нее изменения должны передаваться в другие базы данных (например, если отдел сбыта изменяет цену на определенную продукцию).
- В приложениях, используемых торговыми агентами или представителями для автономной работы на переносных компьютерах, если внесенные ими изменения должны передаваться на центральный сервер при очередном подключении их компьютеров к сети.
- Для организации в Web группы пользователей с помощью приложения, позволяющего благодаря функции подписки периодически извлекать через Internet сведения об изменениях в общей базе данных.
- В распределенных вычислительных средах, в которых серверы импортируют информацию из файлов с ее дальнейшей репликацией на другие узлы.

Публикация и подписка

В системе репликации SQL Server используются понятия публикация (publish) и подписка (subscribe). Серверы системы публикуют свои данные (публикации), на которые могут подписаться другие серверы. В среде SQL Server сервер, который делает свои данные доступными для подписки со стороны других серверов, называется публикующим.

Публикации и статьи

Публикующий сервер предоставляет набор из одной или более статей, называемый публикацией (publication). Публикация, включает выбранные таблицы. Термин статья (article) используется по отношению к базовым объектам репликации, которые могут представлять собой отдельную таблицу, некоторую часть таблицы или хранимые процедуры.

Каждая публикация может содержать один или более перечисленных ниже элементов.

- Таблица.
- Вертикальное разделение таблицы.
- Данные хранимой процедуры (новая функция в SQL Server 2000).
- Горизонтальное разделение таблицы.
- Горизонтальное и вертикальное разделение таблицы

Вертикальное разделение таблицы представляет собой статью, в определении которой используется фильтр, выделяющий в таблице только заданные столбцы.

Горизонтальное разделение таблицы представляет собой статью, в определении которой используется фильтр, выделяющий в таблице только заданные строки данных.

Однако существуют объекты, которые не могут публиковаться.

- Базы данных model, tempdb и msdb.
- Системные таблицы, расположенные в базе данных master.

Типы подписки

Сделанные на публикующем сервере изменения рассылаются подписчикам с помощью механизмов репликации по запросу или принудительно. При осуществлении репликации методом принудительной подписки публикующий сервер организует рассылку подписчикам всех изменений, не ожидая поступления от них запросов на получение информации о выполненных изменениях. Репликация методом принудительной подписки обычно используется в тех случаях, когда желательно сразу же получать извещения обо всех изменениях, выполненных в публикуемой базе данных, либо если требуется гарантировать в системе максимальный уровень безопасности.

При выполнении репликации по запросу подписчик сам инициализирует процесс репликации на стороне публикующего сервера. Репликация по запросу обеспечивает меньший уровень загрузки системы по сравнению с репликацией методом принудительной подписки и больше подходит в тех случаях, когда в системе существует множество подписчиков или требования к уровню безопасности относительно невысоки.

Роли серверов

В общей схеме процессов репликации системы SQL Server каждый сервер может выполнять одну или более перечисленных ниже ролей.

- Публикующий сервер (publisher) содержит исходную базу данных, обеспечивает доступность ее данных для репликации и пересылает сведения о выполненных изменениях в базу данных рассылки, откуда они будут разосланы всем

серверам-подписчикам.

- Сервер-подписчик (subscriber) получает и обрабатывает публикуемые данные.

На стороне подписчика в публикуемую информацию также могут вноситься изменения. Однако в подобных случаях подписчик сохраняет свой статус, а не

становится публикующим сервером. (Любая информация в системе может публиковаться только одним-единственным сервером.)

- Рассылающий сервер (distributor) содержит базу данных рассылки и отвечает

за хранение и пересылку адресатам информации о синхронизации и репликации транзакций. Назначение рассылающего сервера — доставка на все серверы-

подписчики информации, поступающей в его базу данных рассылки от публикующих серверов.

Любой сервер в системе может выполнять одну или более перечисленных ролей. Например, во многих случаях публикующий сервер одновременно является рассылающим и может выступать в роли подписчика по отношению к публикациям, предоставляемым другими публикующими серверами. В последнем случае сервер, функционирующий в системе как публикующий и рассылающий, является и сервером-подписчиком.

Нет ничего необычного в том, что сервер-подписчик одновременно играет роль публикующего сервера. Однако в системе репликации SQL Server установлено, что для каждой публикации может существовать лишь одна ведущая копия базы данных, поддерживаемая публикующим сервером, независимо от числа серверов-подписчиков, которым предоставлено право вносить изменения в данную публикацию. Например, в системе с репликацией методом слияния сервер А публикует базу данных pubs. Серверы В и С являются подписчиками и имеют право вносить в эту базу данных изменения. Ведущая копия базы данных, в которую будут поступать сведения обо всех изменениях, находится на публикующем сервере А. Изменения, выполненные на сервере С, поступят на сервер В после репликации через сервер А.

Внешние системы, отличные от SQL Server (например, Oracle и Microsoft Access), могут выступать в качестве подписчиков для всех существующих типов репликации (за исключением непосредственно обновляемых подписчиков). Кроме того, Microsoft предоставила разработчикам

открытый интерфейс службы репликации транзакций системы SQL Server. В результате третьи фирмы получили возможность создавать программные продукты, позволяющие отличным от SQL Server системам выступать в качестве гетерогенных источников публикуемой информации.

Типы репликации

SQL Server 2000 поддерживает несколько типов репликации, которые могут использоваться в самых разнообразных бизнес-приложениях. В последующих главах детально рассматривается каждый из существующих типов репликации, а также даются рекомендации о том, где и когда он может применяться. В SQL Server поддерживается несколько типов репликации, которые описаны ниже.

Репликация транзакций

В схеме репликации транзакций публикации модифицируются на узле публикующего сервера, после чего сведения о внесенных изменениях рассылаются всем подписчикам на данную публикацию. Репликация транзакций поддерживается в SQL Server, начиная с версий 6.x.

Суть этой схемы состоит в том, что подписчики на публикацию не могут вносить в нее изменений и имеют доступ к содержащейся в ее статьях информации только для чтения. Однако это не означает, что все изменения в публикуемые таблицы могут вноситься только на одном узле. Используя вертикальные и горизонтальные разделения одной и той же таблицы, можно построить модель, в которой данные этой таблицы будут модифицироваться сразу на нескольких узлах. Идея состоит в выделении разделов таким образом, чтобы каждому из узлов было предоставлено право модифицировать собственный раздел данных, публикуемый этим узлом.

SQL Server позволяет организовать двунаправленную репликацию транзакций и без выделения разделов, для чего применяются пользовательские хранимые процедуры и выделение обратных циклов. Однако чаще всего репликация транзакций используется в тех случаях, когда подписчикам достаточно иметь доступ к публикациям только для чтения или можно ограничиться выделением для них собственных разделов данных. Подобные схемы позволяют избежать конфликтов доступа или потери выполненных изменений в системе. Примерами приложений и сценариев, в которых может успешно использоваться схема репликации транзакций, являются базы данных для хранения резервной копии информации, хранилища информации, базы данных с информацией отдельных филиалов или подразделений, центральные базы данных с информацией о складских запасах или объеме реализации, обновляемые и реплицируемые на различные узлы.

Синхронизация

Репликация посредством синхронизации предусматривает фиксацию в конкретный момент времени текущего состояния и структуры данных публикации с последующей рассылкой этих сведений в адрес подписчиков. Синхронизация также впервые появилась в SQL Server 6.x и является имеющим наиболее простую организацию типом репликации. Поскольку передаваемые данные представляют собой копию информации на определенный момент времени, нет необходимости беспокоиться о возникновении конфликтов или потере сведений об отдельных транзакциях. Примерами приложений и сценариев, в которых может успешно использоваться схема синхронизации, являются справочные таблицы, содержимое которых изменяется относительно редко, анонимные подписчики, таблицы со статической или редко изменяемой информацией.

Репликация методом слияния

Репликация методом слияния представляет собой специфическую форму репликации транзакций. Основное отличие этого типа репликации состоит в том, что несколько пользователей могут подписаться на публикацию и независимо редактировать ее статьи (таблицы) без необходимости выполнять разделение данных или применять пользовательские хранимые процедуры. Когда подписчик вносит изменения в публикацию, сведения об этих изменениях пересылаются назад, на публикующий сервер. Если в процессе работы возникает конфликт (например, пользователи на различных узлах модифицируют одну и ту же строку таблицы после синхронизации баз данных), он разрешается либо с помощью приоритетов, либо путем предоставления преимущества первому из пользователей, внесших изменения в данные.

Примерами приложений и сценариев, в которых может успешно применяться схема репликации методом слияния, служат приложения, используемые торговыми агентами на портативных

переносных компьютерах для ввода сведений о заказах и заказчиках в автономном режиме. Позднее, когда агент возвращается в свой офис и подключает переносной компьютер к корпоративной сети, SQL Server обеспечивает передачу данных о выполненных операциях в центральную базу данных.

Непосредственно обновляемые подписчики

Это еще одна форма репликации изменений в SQL Server 2000. Непосредственно обновляемые подписчики организуются на основе репликации транзакций (можно использовать и репликацию синхронизацией) и допускают внесение подписчиком изменений в статьи публикации. Выполненные изменения дублируются на стороне публикующего сервера с помощью двухступенчатого протокола фиксации изменении, а затем реплицируются в адрес остальных подписчиков с использованием стандартного механизма репликации транзакций. Двухступенчатый протокол фиксации изменений требует, чтобы изменение было немедленно выполнено на всех участвующих в транзакции серверах, иначе транзакция будет отменена с восстановлением всех внесенных изменений. Следовательно, все серверы, участвующие в выполнении транзакции, должны иметь надежное соединение друг с другом.

При использовании репликации по схеме непосредственно обновляемых подписчиков удается избежать чрезмерной сложности двухступенчатого протокола фиксации изменений (связанной с необходимостью установки соединений одновременно между всеми участвующими в транзакции серверами), обеспечивая в то же время целостность выполняемой транзакции. Примерами приложений и сценариев, в которых может успешно использоваться репликация по схеме непосредственно обновляемых подписчиков, служат приложения, применяющие надежные сетевые соединения и имеющие невысокий уровень интерактивных транзакций, а также приложения, в которых одни и те же данные обрабатываются как на центральном, так и на удаленных узлах.

Согласованность транзакций

В контексте репликации данных согласованность транзакций означает, что на всех узлах данные будут иметь идентичные состояния, соответствующие тому, которое могло возникнуть при выполнении всех транзакций на одном и том же узле. Репликация вносит в процессы некоторый элемент случайности, который выражается в появлении определенных временных задержек между моментом выполнения изменения в данных и моментом репликации этих сведений подписчикам. В SQL Server 2000 задержки репликации относятся к одному из двух возможных вариантов согласованности транзакций: гарантированной неполной согласованности (guaranteed loose consistency) и гарантированному отсутствию согласованности (guaranteed no consistency).

Гарантированная неполная согласованность означает, что синхронизация данных между сервером-источником и сервером-получателем не выполняется немедленно. Прежде чем подробнее остановиться на этом варианте, рассмотрим еще одну модель распределенных данных — гарантированную точную согласованность (guaranteed tight consistency). Она может быть реализована в SQL Server с использованием двухступенчатого протокола фиксации изменений. В этой модели все выполняемые транзакции либо фиксируются, либо отменяются одновременно на всех серверах, поэтому данные всех серверов всегда синхронизированы на 100%.

В модели с гарантированной неполной согласованностью транзакции фиксируются или отменяются только на исходном сервере. После завершения транзакции сведения о выполненных изменениях асинхронно рассылаются на серверы-подписчики. Самое большое различие между моделями гарантированной точной и гарантированной неполной согласованности данных заключается в том, что в последнем случае между выполнением изменений на исходном сервере и их репликацией на сервер-подписчик проходит некоторое время, на протяжении которого базы данных остаются несогласованными. Модель гарантированной неполной согласованности данных реализуется в функциях репликации транзакций и синхронизации. Модель, реализуемая в функции непосредственно обновляемых подписчиков, можно считать промежуточной между моделями гарантированной точной и гарантированной неполной согласованности данных. В этом случае двухступенчатый протокол фиксации изменений (точная согласованность) используется при взаимодействии серверов двух узлов (публикующий сервер и подписчик), после чего запускается меха-

низм стандартной репликации транзакций (неполная согласованность), применяемый для передачи сведений об изменении в адрес всех остальных подписчиков.

При репликации методом слияния используется модель гарантированного отсутствия согласованности данных. Если согласованность отсутствует, данные идентичны на всех узлах и соответствуют состоянию, которое не может быть получено при выполнении всех транзакций на одном и том же узле.

Поскольку репликация методом слияния предназначена для узлов, не имеющих постоянного соединения друг с другом, возможность автономной работы узла оказывается более важным условием, чем согласованность транзакций. В конце концов состояния данных всех узлов синхронизируются, однако это может оказаться не то состояние, которого можно достичь, если все изменения выполняются на одном и том же узле.

База данных рассылки

В базе данных рассылки хранятся сведения обо всех транзакциях, подлежащих репликации на серверы-подписчики (при использовании репликации транзакций). Она функционирует как промежуточная пересылающая база данных. Сведения о транзакции сохраняются в базе данных рассылки до тех пор, пока все подписчики не подтвердят успешную доставку этой информации. К тому же эта база данных используется для хранения информации о синхронизации публикаций и подписчиков.

Системные таблицы, входящие в состав базы данных рассылки.

- MSmerge_history — содержит информацию о выполненных ранее обновлениях подписчиков.
- MSmerge_agents — содержит сведения об агентах слияния.
- MSdistribution_agents — содержит сведения об агентах рассылки.
- MSdistribution_history — содержит информацию для агентов рассылки.
- MSlogreader agents — содержит сведения об агентах чтения журнала на локальном рассылающем сервере.
- MSlogreader_history — содержит информацию для агентов чтения журнала.
- MSrepl_commands — содержит команды репликации.
- MSrepl errors — содержит сведения о неудачных попытках выполнения процедур репликации.
- MSrepl_transactions — содержит отдельную строку для каждой подлежащей репликации транзакции.
- MSrepl version — содержит единственную строку со сведениями о версии текущей установленной службы репликации.

Обзор агентов репликации SQL Server

Для эффективного управления работой системы репликации SQL Server необходимо подробно ознакомиться с различными агентами, используемыми в процессах репликации.

Все существующие типы агентов:

- Агент чтения журнала (log reader). Анализирует наличие в журнале транзакций публикуемой базы данных записей об отдельных транзакциях, подлежащих репликации. Сведения о найденных транзакциях агент чтения журнала помещает в базу данных рассылки. Во всех публикациях по методу репликации транзакций имеются агенты чтения журнала.
- Агент слияния (merge agent). Отвечает за слияние поступающих изменений, а также за выполнение исходной синхронизации, осуществляемой с помощью агента синхронизации.
- Агент синхронизации (snapshot agent). Создает файлы синхронизации на рассылающем сервере и фиксирует в базе данных рассылки статус информации о синхронизации между публикуемой базой данных и базами данных серверов-подписчиков. Во всех публикациях имеются агенты синхронизации.
- Агент рассылки (distribution agent). Отвечает за рассылку серверам-подписчикам сведений о транзакциях, помещенных в базу данных рассылки.

В публикациях по методу репликации транзакций и синхронизации имеются отдельные агенты рассылки для каждого сервера-подписчика.

В SQL Server 2000 с помощью предоставляемых элементов управления ActiveX агенты слияния и рассылки могут быть запущены из других приложений.

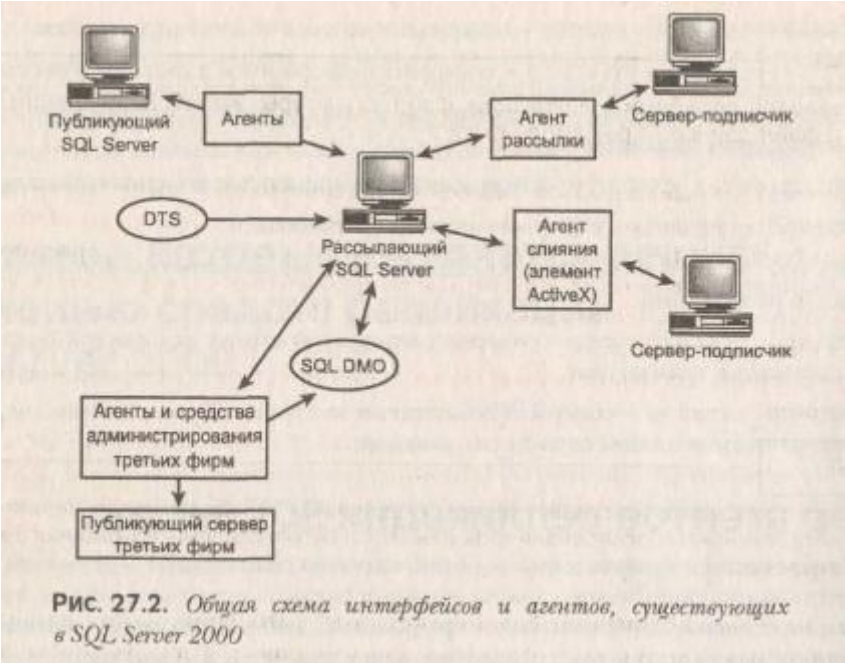



**Рис. 27.2.** *Общая схема интерфейсов и агентов, существующих в SQL Server 2000*

Варианты согласования

Согласованием (synchronization) называется процесс уведомления публикующего сервера и сервера-подписчика о том, что их базы данных находятся в одном состоянии и службы репликации могут начать свою работу. SQL Server поддерживает несколько вариантов согласования. По умолчанию используется автоматическое согласование серверов, означающее, что система SQL Server автоматически выполняет процедуры согласования в соответствии с установленным интервалом. Если согласование не выполняется, SQL Server предполагает, что статьи источника данных уже синхронизированы со статьями серверов-получателей. Система не предпринимает никаких действий для подтверждения этого факта. В таком случае вся ответственность возлагается на администратора.

**Возможности командных файлов MS-DOS**

Введение

Довольно часто в процессе работы с компьютером обнаруживается, что необходимо повторять одни и те же команды MS-DOS (может быть, с небольшими изменениями) для того, чтобы осуществить некоторые периодически выполняемые действия. Операционная система MS-DOS позволяет записать нужную для этого последовательность команд в специальный текстовый файл, называемый командным файлом. Командный файл должен иметь расширение .bat. Командные файлы часто называются пакетными файлами. Именно по расширению .bat командные файлы отличается операционной системой от файлов других типов. Последовательность команд, записанную в файле, можно выполнить, набрав имя пакетного файла (расширение .bat при этом можно не указывать).

Пример. Для удаления ненужных файлов и оптимизации размещения файлов на жестком диске (иначе говоря, “сжатия” диска) можно использовать такую последовательность команд:

| | |
|---|---|
| C: | – Переход на диск C:. |
| Cd\ | – Переход в корневой каталог. |
| Del Temp*.* | – Удаление временных файлов в каталоге |

Defrag C: /f ‘C:\Temp’.
– Дефрагментация диска C:.

Чтобы не набирать каждый раз эти команды вручную, запишем их в текстовый файл, располагая каждую команду на отдельной строке. Данный файл назовем ‘Compact.bat’ и сохраним его в каталоге, где находятся служебные файлы и команды MS-DOS. Если теперь ввести команду ‘Compact’, тогда автоматически выполнится содержащаяся в нем последовательность команд.

1. Выполнение командных файлов

Рассмотрим действия, которые необходимо предпринять для запуска командных файлов, а также то, как они выполняются операционной системой MS-DOS.

1. Для выполнения пакетного файла, находящегося в текущем каталоге или в одном из каталогов, указанных в команде Path файла Autoexec.bat, выполняемого при загрузке MS-DOS, достаточно просто ввести имя этого файла и параметры, отделенные друг от друга пробелами. Расширение имени командного файла (т.е. .bat) можно не указывать.

2. Для выполнения пакетных файлов, не находящихся в текущем каталоге или в одном из каталогов, указанных в команде Path, следует обязательно указывать полный путь к каталогу, в котором находится пакетный файл, его имя и передаваемые ему параметры. Общий вид команды вызова пакетного файла будет таким:

(диск:) (\путь\) имя-командного-файла ($пар_1$ $пар_2$ … $пар_k$)

Здесь $пар_1$ $пар_2$ … $пар_k$ – параметры командного файла.

Пример. Пусть текущий каталог – ‘C:\Doc\Work’, а надо выполнить командный файл ‘Account.bat’, находящийся в каталоге ‘C:\Doc\Batch’, и указать ему два параметра: ‘Bill.doc’ и ‘/P’. Для выполнения этого пакетного файла нужно ввести следующую команду:

C:\Doc\Batch\Account Bill.doc /P

или команду

..\Batch\Account Bill.doc /P

3. Выполнение командного файла можно прервать, нажав комбинацию клавиш Ctrl + C или Ctrl + Break . После этого на экране появится запрос:

Terminate batch job (Y/N)?

который означает

Прервать выполнение пакетного файла (Да/Нет)?

Если ответить Y то выполнение пакетного файла будет окончено, а оставшиеся невыполненные команды будут проигнорированы. Если ответить N , то выполнение пакетного файла будет продолжено.

4. Если вынуть дискету, на которой расположен выполняемый в данный момент командный файл, то перед выполнением следующей команды MS-DOS попросит снова вставить эту дискету в дисковод.

5. Из одного командного файла можно вызвать другой командный файл, просто указав его имя (и, если надо, полный путь к нему и параметры). Однако после окончания работы вызванного файла выполнение исходного командного файла продолжено не будет. Если требуется выполнить другой командный файл, а затем продолжить выполнение исходного командного файла, тогда следует использовать команду Call .

6. В MS-DOS, начиная с версии 6.2, возможно вызвать пакетный файл в пошаговом режиме. Это может быть очень удобно для его отладки. Формат команды:

Command /Y /C имя-командного-файла (параметры)

Текст каждой команды будет выводиться перед выполнением на экран. Для выполнения команды надо нажать клавишу Y или Enter , для пропуска команды - N или Esc .

2. Вызов командных файлов с возвратом. Команда Call

Если из командного файла вызвать другой командный файл, вставив в него имя этого командного файла с необходимыми параметрами, то после завершения вызванного файла возврата управления в исходный командный файл не произойдет. Если же такой возврат необходим, следует использовать команду Call. Формат команды:

Call имя-командного-файла (параметры)

Команда Call вызывает выполнение командного файла из другого командного файла. Если в командной строке указаны какие-либо параметры, кроме имени командного файла, то эти параметры передаются командному файлу, они доступны по символическим именам %1 - %9. После завершения вызванного командой Call командного файла выполнение исходного командного файла продолжается со следующей после нее команды.

Замечание. В команде Call не допускается перенаправление ввода-вывода (т.е. использования символов ‘<’, ‘>’ и ‘|’).

3. Параметры в командных файлах

3.1. Общие сведения

Часто приходится выполнять одни и те же команды или последовательности команд MS-DOS с весьма небольшими отличиями. Например, для трансляции программы на Фортране с помощью транслятора фирмы Microsoft надо набирать команды типа:

fl /4I2 /AL /Ox /PP187 /c имя-файла

Чтобы упростить вызов транслятора, можно создать файл Fort.bat следующего содержания:

fl /4I2 /AL /Ox /PP187 /c %1

Здесь символическое имя %1 означает первый параметр, указанный при вызове пакетного файла. Например, если ввести команду ‘Fort Simpson.for’, тогда вместо %1 будет подставлено ‘Simpson.for’ и тем самым будет выполнена команда:

fl /4I2 /AL /Ox /PP187 /c Simpson.for

3.2. Символические имена параметров командного файла

В командном файле одновременно можно иметь доступ к девяти параметрам, которые обозначаются как %1, %2, ..., %9. Если при вызове командного файла задано меньше девяти параметров, тогда “лишние” символические имена в качестве значений хранят в себе пустые строки. Если нужно обработать в командном файле более девяти параметров, тогда следует применить в нем команду Shift.

Символическое имя %0. В командном файле можно использовать также символическое имя %0, в котором изначально хранится имя выполняемого командного файла (в той форме, в которой оно указано в команде, вызвавшей данный командный файл).

Использование символа %. Если в командном файле знак процента используется не для обозначения параметров, а для других целей, то его надо набрать дважды. Так, чтобы в командном файле указать файл ‘xyz%.com’, надо написать в нем строку ‘xyz%%.com’.

3.3. Команда Shift

Иногда в командном файле требуется применить более девяти параметров, либо выполнить одинаковую обработку для всех параметров командного файла. В этих случаях следует использовать команду Shift. Если она встречается в командном файле, тогда символические имена его параметров приобретают новые значения: в %0 попадет прежнее значение из %1, в %1 – прежнее значение из %2 и т.д. В %9 будет помещено значение десятого параметра из командной строки, а если он не задан, тогда новое значение %9 - пустая строка. Команду Shift можно использовать несколько раз.

Пример. Пусть командный файл ‘Dummi.bat’ вызван следующей командной строкой:

Dummi a bb ccc

Тогда %0 = ‘Dummi’, %1 = ‘a’, %2 = ‘bb’, %3 = ‘ccc’, а параметры с %4 по %9 содержат пустые строки. После однократного выполнения команды Shift имеем: %0 = ‘a’, %1 = ‘bb’, %2 = ‘ccc’, а параметры с %3 по %9 содержат пустые строки.

4. Переменные среды MS-DOS и работа с ними в командных файлах

4.1. Общие сведения

Операционная система MS-DOS имеет специальную область памяти, называемую средой или окружением (от англ. environment), в которой хранится набор символьных строк, доступных во всех программах и командных файлах. Каждая строка в окружении MS-DOS имеет вид:

имя-переменной = значение,

Здесь имя-переменной - это строка символов, без знаков равенства и пробелов, а значение – любая строка символов.

4.2. Доступ к переменным среды MS-DOS в командном файле

Для установки переменных окружения в командных файлах используется команда Set. Формат команды:

Set переменная = значение

При выполнении этой команды MS-DOS преобразует в имени переменной, но не в ее значении, все строчные буквы в заглавные.

В командных файлах можно обратиться к значению какой-либо переменной окружения, для этого следует указать ее имя, обрамленное с обеих сторон знаками процента.

Пример №1. Для вывода на экран значения переменной окружения Temp в командном файле можно воспользоваться такой командой:

Echo %Temp%

Пример №2. Чтобы удалить все временные файлы в каталоге, заданном в переменной окружения Temp, в командном файле можно воспользоваться такой командой:

Del %Temp%*.*

5. Управление отображением команд на экране

5.1. Команды ‘Echo on’ и ‘Echo off’

По умолчанию команды пакетного файла выводятся на экран перед выполнением. Если в него вставить команду ‘Echo off’, тогда выполняемые за ней команды не будут выводиться на экран. Команда ‘Echo on’ включает режим вывода выполняемых команд на экран. Команда Echo без параметров выводит на экран сообщение о том, включен или выключен режим дублирования команд на экран.

5.2. Командный префикс @

Можно избежать вывода (дублирования) на экран любой отдельной строки командного файла. Для этого надо поставить в начале этой строки символ ‘@’. В частности, можно избежать выдачи на экран команды ‘Echo off’, поставив перед ней символ ‘@’: ‘@Echo off’.

Замечания:

1. Обычно в качестве первой строки командного файла используется команда ‘@Echo off’. При этом строки командного файла на экран не выводятся.

2. После выдачи команды ‘@Echo off’ иногда полезно использовать команду Cls – “очистка экрана”, чтобы сделать более удобным просмотр сообщений, выводимых из командного файла.

6. Вывод сообщений в командных файлах

6.1. Команда Echo

Данная команда позволяет выдавать из командного файла сообщения на экран. Формат команды:

Echo сообщение

Указанное сообщение выводится на экран даже тогда, когда режим вывода исполняемых команд на экран выключен командой ‘Echo off’. Сообщение не может быть пустым или равным зарезервированному слову ‘on’ или ‘off’, так как команды ‘Echo on’ и ‘Echo off’ управляют режимом вывода исполняемых команд на экран, а команда Echo без параметров сообщает, включен или выключен режим дублирования команд на экран.

Замечания.

1. В сообщении не следует употреблять символов ‘<’, ‘>’ и ‘|’ - они интерпретируются как символы перенаправления ввода-вывода.

2. Перед командой ‘Echo сообщение’ желательно выполнить команду ‘@Echo off’, чтобы сообщение не выводилось на экран дважды.

6.2. Получение звукового сигнала

С помощью команды Echo можно получить звуковой сигнал компьютера. Для этого следует в выводимое сообщение включить символ с кодом 7. Это можно сделать, нажав клавишу Alt и, не отпуская ее, клавишу $7_{\text{Home}}$ в правой части клавиатуры.

6.3. Вывод пустой строки

Чтобы вывести на экран пустую строку, а это может понадобиться для повышения удобочитаемости сообщений, можно использовать команду:

Echo.

Точка должна следовать сразу за словом ‘Echo’. Другой вариант - вывести сообщение, состоящее из одного символа с кодом 255, который при выводе на экран никак не отображается.

6.4. Вывод сообщений в файл

С помощью символа перенаправления ввода-вывода ‘>’ можно выводить сообщения не на экран, а в файл.

Для добавления строки с сообщением в конец файла следует применить такую команду:

Echo сообщение>> имя-файла

Замечание. Если файл не существует, тогда он создается.

Для создания файла и запись в него строки с сообщением нужно применить такую команду:

Echo сообщение> имя-файла

Замечание. Если указанный файл уже существует, то его старое содержимое будет потеряно.

## 2. Методические рекомендации (указания) к практическим занятиям

**Инструменты анализа сетевых подключений.**

1. Используя терминальную программу, подключитесь к учебному серверу. (В качестве терминала используйте Internet Explorer, указав адрес http://<адрес>/tsweb.
2. Для первоначального входа используйте параметры: Имя пользователя: Фамилия ИО, Пароль: stud. (при первом входе ОС попросит сменить пароль).
3. Запустите справку по ОС Windows. Найдите раздел, относящийся к использованию командной строки, и просмотрите синтаксис команды, какие функции выполняют различные ключи.
4. Выполните команду cmd /f:on. Пролистайте с помощью функции завершение имен файлов содержимое диска d:. Создайте на диске d: собственный каталог (d:\каталог группы\имя). Сделайте собственный каталог текущим.
5. Просмотрите с помощью справочной системы назначение команд: netstat, ping, pathping, tracert, ipconfig, route.
6. Используя перечисленные команды выведите информацию и сохраните в файлах:
   a. Об активных текущих подключениях (в файл connect.txt);
   b. Таблицу зарегистрированных маршрутов (traceroute.txt);
   c. Информацию о настройках протокола IP на сетевой карте (netconfig.txt);
   d. Информацию о проверке сетевого соединения с узлом www.ru (www.txt);
   e. Информацию о латентности сети и потерях данных на промежуточных узлах между исходным пунктом и пунктом назначения. (trace.txt).
7. Просмотрите с помощью справочной системы синтаксис команд net.
8. Выводите список общих ресурсов на собственном компьютере, на компьютерах окружения.
9. Отправьте сообщение «Привет, коллега» пользователю на соседнем компьютере.
10. Выведите информация о конфигурации службы server и workstation. Выведите информацию о текущих подключениях к серверу.
11. Используя терминальную программу, подключитесь к учебному серверу. (В качестве терминала используйте Internet Explorer, указав адрес http://<адрес>/tsweb. Для первоначального входа используйте параметры созданной Вами учетной записи.
12. Выведите информацию обо всех общих ресурсах компьютера (сервера).
13. Используя команду net share откройте для общего доступа вашу папку под именем Папка ваше имя. Установите ограничение на подключение не более 5 пользователей.
14. Просмотрите с сервера общие ресурсы на Вашем локальном компьютере. Подключите общую папку соседнего компьютера в качестве диска F:. Просмотрите содержимое сетевого диска.
15. В завершение задания, отключите общие сетевые ресурсы.
16. Просмотрите справку по ключам команд arp и ping.
17. Запустите режим работы с командной строкой. Используя редактор edit, создайте файл arpping.exe. Введите следующую информацию

```
rem arpping.bat
ping –n 1 –l 1 %1.%2
arp –a %1.%2
```

Сохраните файл, попробуйте запустить данный пакетный файл, задав необходимые параметры командной строки. Первый параметр определяет адрес сети, второй параметр адрес хоста.

17. Просмотрите с помощью справочной системы синтаксис команды for. Создайте с помощью редактора edit командный файл test.bat, включив в него следующую информацию:

```
rem test.bat
for /l %%i in (2,15,254) do arpping 192.168.160 %%i
```

Сохраните файл, проверьте его исполнение. Исправьте файл таким образом, чтобы тестировались хосты в вашем компьютерном классе (необходимо узнать начальный и конечный адреса).

18. Запустите исправленный файл test.bat таким образом, чтобы информация о адресах сохранилась в файле arptest.txt.

19. Просмотрите справку о командах netsh. Команды сетевой диагностики Netsh (diag) используются для управления и устранения неполадок операционной системы и параметров сети из командной строки. Для сетевой диагностики Netsh используется командная строка netsh diag>.

20. Используя параметры команды, протестируйте:

a. Подключение к прокси-серверу

b. Подключение к хосту 212.30.160.7 по портам 25, 80, 110, 10, просмотрите результат

c. Соединение с dns-серверами

d. Соединение со шлюзом по умолчанию

e. Выведите информацию о всех сетевых клиентов, определенных для адаптера.

f. Вывод сведений о локальной операционной системе.

g. Выполните отображение всех сетевых объектов локального компьютера и проверка наличия связи с каждым объектом с помощью команды ping.

21. Используя параметры команды netsh interface выведите информацию о текущих настройках системы.

22. Просмотрите назначение команды nbtstat. Выведите информацию о текущих сеансах.

23. Просмотрите назначение команды tasklist. Выведите информацию о запущенных приложениях на сервере.

24. Используя команду sc, просмотрите информацию о запущенных на компьютере службах. Просмотрите параметра службы Рабочая станция (lanmanworkstation).

25. Добавьте оснастку Службы в консоль MyConsole.msc. Откройте список служб и сравните параметры отображаемые в окне консоли и через командную строку.

26. Закройте все окна и завершите сеанс удаленной работы.

**Работа в командной строке.**

1. Используя терминальную программу, подключитесь к учебному серверу. (В качестве терминала используйте Internet Explorer, указав адрес http://<адрес>/tsweb. Для первоначального входа используйте параметры созданной Вами учетной записи.

2. Используя параметры команды cmd измените цвет шрифта и фона в окне с командным процессором.

3. Используя справку, просмотрите синтаксис команды prompt. Используя ключи команды, установите приглашение в командной строке Доброе утро Собственное имя, уже время, пора начинать работать>

4. Просмотрите в справочной системе Windows синтаксис команд set, echo. Используя данную команды, выведите в файл def.txt список переменных, заданных в текущем сеансе ОС. Создайте переменные %firstname% и %lastname% и присвойте им собственные имя и фамилию. Создайте переменную %fullname%, в которой использовались бы обе эти переменные. С помощью команды echo проверьте корректность значения переменной %fullname%.

5. Просмотрите в справочной системе Windows синтаксис команд dir. Используя ключи команды, попробуйте найти самый большой файл на диске e:. В каком каталоге он размещен.

6. Используя команду systeminfo, выведите информацию сводную информацию о системе в файл systeminfo.txt. Просмотрите содержимое файла.

7. С помощью команды driverquery, выведите список драйверов, загруженных в систему в файл listdriver.txt. Изменив ключи команды, просмотрите список подписанных драйверов.

8. С помощью команды query session просмотрите список пользователей, подключенных к серверу. Каковы параметры подключений?

9. Просмотрите формат команды reg query. Создайте пакетный файл ListReg.bat и внесите следующие команды:

```
reg query HKLM\HARDWARE\DESCRIPTION\System /v SystemBiosVersion
reg query HKLM\HARDWARE\DESCRIPTION\System /v SystemBiosDate
reg query HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0
```

10. Запустите командный файл. Просмотрите информацию и сравните ее с данными из реестра, отображаемые в редакторе реестра (для запуска редактора, введите команду regedit).

11. Создайте в Блокноте файл сценария first.vbs и внесите следующие данные:

```
Option Explicit
On Error Resume Next
Dim FolderPath ' folder to be searched for files
Dim objFSO
Dim objFolder
Dim colFiles
Dim objFile

FolderPath = "C:\inetpub\wwwroot"
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFolder = objFSO.GetFolder(FolderPath)
Set colFiles = objFolder.Files

For Each objFile in colFiles
   Wscript.Echo objFile.Name, objFile.Size & " bytes"
      WScript.Echo VbTab & "created: " & objFile.DateCreated
   WScript.Echo VbTab & "modified: " & objFile.DateLastModified
Next
```

12. Запустите сценарий с помощью команды cscript first.vbs. Просмотрите результаты. Выполните запуск сценария с помощью wscript (для этого достаточно дважды щелкнуть по пиктограмме файла сценария в окне Проводника).

13. Завершите сеанс работы с сервером.

**Администрирование БД средствами SQL Server 2000**

Задание 1. Просмотр свойств файлов данных и журналов транзакций

1. Используя SQL Server Enterprise Manager, подключитесь к учебному экземпляру SQL Server.
2. Откройте контейнер Databases и выберите базу данных db444.
3. Используя контекстное меню, определите свойства файлов БД:
- логическое имя БД,
- физическое имя файла БД,
- его место расположения на диске,
- объем занимаемый БД на диске.
4. Определите пользователей СУБД, имеющих право работать с данной БД, их права.
5. Используя закладку Transaction Log, определите свойства журнала транзакций:
- логическое имя журнала транзакций;
- физическое имя файла журнала транзакций;
- его месторасположения на диске;
- объем занимаемый журналом на диске.
6. Определите, какая модель восстановления выбрана для данной БД.

Задание 2. Непосредственные запросы к системным таблицам

1. Используя SQL Server Query Analyzer, подключитесь к учебному экземпляру SQL Server. Для этого необходимо указать имя экземпляра в окне Connect To SQL Server. Используйте режим проверки подлинности Windows.
2. В окне запросов введите SELECT * FROM sysdatabases, запустите запрос. В окне результатов запроса отобразится информация о каждой БД (идентификатор БД – dbid, идентификатор защиты – sid владельца БД, дата создания, уровень совместимости, данные о размещении главного файла и настроенные параметры БД).
3. Очистите окно запроса с помощью кнопки Clear Windows или CTRL+SHIFT+DEL.

4. В окне запросов введите SELECT * FROM sysaltfiles, запустите запрос. В окне результатов отобразится информация обо всех файлах данных и журналах транзакций (файловый идентификатор, идентификатор БД, физическое и логическое имя файла, расположение, размер и параметры увеличения размера).

5. Очистите окно запроса с помощью кнопки Clear Windows или CTRL+SHIFT+DEL.

6. В окне запросов введите SELECT * FROM syslogins, запустите запрос. В окне результатов отобразится информация обо всех учетных записях: идентификатор защиты – sid, идентификатор учетной записи, зашифрованный пароль, БД по умолчанию, роль сервера.

7. Очистите окно запроса с помощью кнопки Clear Windows или CTRL+SHIFT+DEL.

8. В окне запросов введите SELECT * FROM sysusers, запустите запрос. В окне результатов отобразится информация обо всех пользователях и группах пользователях, роли в БД: идентификатор пользователя, идентификатор группы – gid, дату создания.

9. Закройте SQL Query Analyzer, не сохраняя изменений.

Задание 3. Выполнение запроса к системным таблицам средствами системных хранимых процедур

1. Используя SQL Server Query Analyzer, подключитесь к учебному экземпляру SQL Server. Для этого необходимо указать имя экземпляра в окне Connect To SQL Server. Используйте режим проверки подлинности Windows.

2. В окне запросов введите имя системной хранимой процедуры sp_helpdb, выполните запрос. В окне результатов запроса отобразится информация обо всех базах данных.

3. Для получения информации о базе данных Db444, укажите ее имя после имени процедуры: sp_helpdb Db444. Просмотрите результаты выполнения процедуры.

4. В окне запроса введите sp_spaceused и выполните запрос.

5. В окне результатов отобразится информация о пространстве занятой текущей БД. Выберите БД Northwind и просмотрите результаты запроса.

6. Для просмотра объема пространства, занятого отдельной таблицей укажите имя таблицы после имени процедуры в одинарных кавычках. В окне Object Browser просмотрите имена пользовательских таблиц и запишите запросы, определяющие размер и число записей для отдельных пользовательских таблиц (customers, region, orders).

7. Очистите окно запроса и введите sp_depends ‘имя объекта БД’, указав в качестве имени одну из пользовательских таблиц БД Northwind.

8. Получите информацию о зависимостях таблицы Employee.

9. Очистите окно запроса и используя системную хранимую процедуру sp_who определите информацию обо всех пользователях и процессах СУБД. Отобразите только активных пользователей, указав ключевое слово active.

10. Закройте SQL Query Analyzer, не сохраняя изменений.

Задание 4. Выполнение запроса к системным таблицам средствами системных функций

1. Используя SQL Server Query Analyzer, подключитесь к учебному экземпляру SQL Server. Для этого необходимо указать имя экземпляра в окне Connect To SQL Server. Используйте режим проверки подлинности Windows.

2. В окне запросов введите SELECT DB_ID(‘Db444’). Системная функция отображаем идентификатор БД.

3. Очистите окно запросов. Введите SELECT DB_NAME(6). Системная функция возвращает имя БД с заданным идентификатором.

4. Очистите окно запросов. Введите SELECT HOST_NAME(). Системная функция возвращает имя хоста.

5. Очистите окно запросов. Введите SELECT FILEPROPERTY(‘Northwind’,’SpaseUsed’). Системная функция возвращает число страниц, занятых БД.

6. Очистите окно запросов. Введите SELECT USER_NAME(2). Системная функция возвращает имя пользователя. Просмотрите имена пользователей для разных БД.

7. Очистите окно запросов. Закройте SQL Query Analyzer, не сохраняя изменений.

Задание 5. Выполнение запроса к системным таблицам средствами представления информационной схемы

1. Используя SQL Server Query Analyzer, подключитесь к учебному экземпляру SQL Server. Для этого необходимо указать имя экземпляра в окне Connect To SQL Server. Используйте режим проверки подлинности Windows.
2. В окне запросов введите SELECT * FROM INFORMATION_SCHEMA.SCHEMATA. Запрос возвратит список БД, доступных пользователю.
3. Очистите окно запросов, введите SELECT * FROM INFORMATION_SCHEMA.TABLES. Запрос возвратит список таблиц текущей БД, доступных текущему пользователю.
4. Очистите окно запросов, введите SELECT * FROM INFORMATION_SCHEMA.TABLE_PRIVILEGES. Запрос возвратит список привилегий предоставленных текущему пользователю и тех, которые он предоставил другим в текущей БД.
5. Очистите окно запросов, введите SELECT * FROM INFORMATION_SCHEMA.COLUMNS Запрос возвратит список полей, доступных текущему пользователю.
6. Закройте SQL Query Analyzer, не сохраняя изменений.

**Администрирование БД средствами SQL Server 2000 (работа 2)**

Задание 6. Создание базы данных с помощью мастера Create Database

1. Используя SQL Server Enterprise Manager, подключитесь к учебному экземпляру SQL Server.
2. С помощью команды меню Tools запустите Wizards, выберите мастер Create Database Wizard.
3. Используя Мастер создайте новую базу данных, задав имя WizardDB_<собственное имя>. В качестве параметров для файла БД установите:
   - начальный размер – 10 Мб;
   - увеличение БД – 10%;
   - ограничит рост БД – 30 Мб;

   В качестве параметров для файла журнала транзакций:
   - начальный размер – 2 Мб;
   - увеличение БД – 1 Мб;
   - ограничит рост БД – 12 Мб;
4. Просмотрите результаты работы Мастера.

Задание 7. Создание базы данных с SQL Server Enterprise Manager

1. Используя SQL Server Enterprise Manager, подключитесь к учебному экземпляру SQL Server.
2. С помощью контекстного меню выполните создание базы данных.
3. Задайте имя базы данных SEMDB_<собственное имя>. В качестве параметров для файла БД установите:
   - начальный размер – 4 Мб;
   - увеличение БД – 2 Мб;
   - ограничит рост БД – 30 Мб;
   - размещение – C:\db\semdb_<имя>_db.mdf

   В качестве параметров для файла журнала транзакций:
   - начальный размер – 2 Мб;
   - увеличение БД – 10%;
   - ограничит рост БД – 10 Мб;
   - размещение – C:\db\semdb_<имя>_log.ldf
4. Просмотрите результаты работы.

Задание 8. Создание базы данных с Transact-SQL

1. Используя SQL Server Enterprise Manager, подключитесь к учебному экземпляру SQL Server.
2. С помощью меню Tools запустите SQL Query Analyzer.
3. В окне запроса запишите следующий запрос:

```
CREATE DATABASE TSQLDB_<имя>
ON
( NAME = TSQLDB_DATA, FILENAME = 'C:\DB\TSQLDB_<имя>.MDF',
  SIZE = 10, MAXSIZE = 25, FILEGROWTH = 5 )
LOG ON
( NAME = TSQLDB_LOG, FILENAME = 'C:\DB\TSQLDB_<имя>.LDF',
  SIZE = 2, MAXSIZE = 12, FILEGROWTH = 25% )
```

4. Просмотрите результаты работы.

**Администрирование БД средствами SQL Server 2000 (работа 3)**

Задание 9. Изменение размера файла данных БД

1. Используя SQL Server Enterprise Manager, подключитесь к учебному экземпляру SQL Server.
2. Выберите собственную БД SEMDB_<собственное имя>, созданную на прошлом занятии.
3. Используя SQL Query Analyzer, сформируйте запрос ALTER DATABASE, отключающий автоматическое увеличение размера основного файла данных БД.
4. Просмотрите изменение в свойствах БД с помощью SQL Server Enterprise Manager.
5. Используя SQL Query Analyzer, сформируйте запрос DBCC SHRINKFILE уменьшающий размер файла данных БД TSQDB_<собственное имя> до 5 Мб.
6. Просмотрите результаты выполнения с помощью SQL Server Enterprise Manager.
7. Выполните операцию увеличения размера файла журнала транзакций БД TSQDB_<собственное имя> до 5 Мб, одновременно отменив автоматическое увеличение.
8. Просмотрите результаты выполнения.
9. Выполните операцию создания дополнительного файла данных к БД SEMDB_<собственное имя>, установив параметры (расположение файла C:\DB\SEMDB2_<собственное имя>.ndf, начальный размер – 5 Мб, максимальный размер – 10 Мб, увеличение – 1 Мб).
10. Отключитесь от учебного экземпляра SQL Server.

Задание 10. Перенос данных в БД посредством мастера DTS Import/Export Wizard

1. Используя SQL Server Enterprise Manager, подключитесь к учебному экземпляру SQL Server.
2. Запустите Мастер экспорта/импорта данных (Export/Import Data в группе программ Microsoft SQL Server).
3. Убедитесь, что в списке Data Source выбран источник данных Microsoft OLE DB Provider for SQL Server.
4. В качестве сервера БД выберите учебный экземпляр SQL Server.
5. Выберите в качестве источника данных БД Northwind
6. Щелкните по кнопке Далее > и перейдите к выбору получателя данных.
7. Убедитесь, что в списке Data Source выбран источник данных Microsoft OLE DB Provider for SQL Server. В качестве сервера БД выберите учебный экземпляр SQL Server.
8. Выберите в качестве получателя данных БД SEMDB_<собственное имя> (если такой БД нет можно выбрать <new> и задать указанное имя).
9. Щелкните по кнопке Далее > и перейдите к заданию объектов копирования.
10. Убедитесь, что переключатель находится в положении Copy Table and View From The Source Database и перейдите к следующему шагу.

11. Для выбора всех объектов щелкните кнопку Select All. Объектам в новой БД по умолчанию будут присвоены такие имена, что и в источнике. Щелкните по кнопке Далее > и перейдите к следующему этапу.

12. На данном шаге указывается параметры расписания (по умолчанию пакет выполняется однократно и немедленно), а также параметры сохранения DTS-пакета.

13. Пометьте флажок Save DTS Package и выберите вариант SQL Server. Перейдите к следующему шагу.

14. В качестве имени укажите <собственное имя>DTSPackageTableCopy и перейдите к завершающему шагу, нажав кнопку Далее >.

15. Просмотрите основные параметры DTS пакета.

16. Выполните пакет, нажав кнопку Готово.

Задание 11. Использование конструктора DTS Designer для импорта и преобразования данных

1. Используя SQL Server Enterprise Manager, подключитесь к учебному экземпляру SQL Server.

2. В дереве консоли SQL Server Enterprise Manager раскройте контейнер Data Transformation Services, выберите Local Packages и найдите пакет, созданный Вами в предыдущем задании.

3. Дважды щелкните по пакету для открытия DTS Designer. Ознакомьтесь со структурой конструктора DTS-пакетов.

4. Просмотрите структуру DTS-пакета. Он включает множество созданий таблиц и переноса данных таблиц из БД Northwind в вашу БД.

5. Найдите преобразование, относящееся к переносу таблицы Products. Щелкните дважды мышью по стрелке Transformation Data Task. Измените SQL запрос, установив требование переноса строк только для Кондитерских изделий (CategoryName = Condiments, CategoryID = 2).

6. Структура SQL_запроса имеет вид:

```
SELECT    ProductID, ProductName, SupplierID, CategoryID, QuantityPerUnit,
UnitPrice, UnitsInStock, UnitsOnOrder, ReorderLevel, Discontinued
FROM      Products
WHERE     (CategoryID = 2)
```

7. Сохраните модифицированный DTS – пакет.

8. Откройте БД sembd_<имя> и удалите все пользовательские таблицы.

9. Запустите собственный DTS – пакет.

10. Просмотрите результаты выполнения. Раскройте содержимое таблицы Products, просмотрите скопированные записи, сравните с содержимым такой же таблицы БД Northwind.

11. Закройте SQL Server Enterprise Manager.

**Администрирование БД средствами SQL Server 2000**

**Автоматизация административных задач**

Задание 1. Создание и назначение надежного оператора.

1. Используя Internet Explorer, подключитесь к удаленному рабочему столу учебного сервера БД.

2. Используя средства Windows, создайте пользователя failsafe_собств_имя на удаленном компьютере.

3. Закройте удаленный рабочий стол.

4. Установите средствами Enterprise Manager соединение с учебным экземпляром SQL Server.

5. Создайте новую БД JobBD_собств_имя, установив в качестве места размещения файлов БД и журнала транзакций папку c:\db\444.

6. Выполните экспорт данных (таблиц, представлений, хранимых процедур) из БД pubs в созданную Вами БД.

7. Выберите контейнер Operators и создайте нового оператора с собственным именем. В поле Net Send установите ваше доменное имя и щелкните кнопку Test.

8. Вызовите Свойства контейнера SQL Server Agent и выберите вкладку Alert System.

9. В группе Fail-Safe Operator выберите – создание нового оператора. В качестве надежного оператора выберите failsafe_собств_имя. Задайте вариант оповещения по сети.

10. Закройте окна Enterprise Manager.

Задание 2. Создание задания посредством мастера Create Job Wizard.

1. Установите средствами Enterprise Manager соединение с учебным экземпляром SQL Server.

2. Выберите в меню Tools команду Wizards, в группе Management найдите и запусите нужный мастер.

3. В качестве типа задания выберите Transact-SQL command и перейдите к следующему шагу.

4. В поле Transact-SQL введите BACKUP DATABASE JobBD_собст_имя TO DISK='C:\DB\444\JobDB_собств_имя.bak'.

5. Щелкните кнопку Parse для проверки синтаксиса команды. Если отсутствуют ошибки, перейдите к следующему шагу.

6. Установите расписание выполнения задания: еженедельно по понедельникам в 9:00.

7. Задайте в качестве оператор собственное имя.

8. Задайте в качестве имени задания Job_собственное_имя.

9. Сохраните задание.

Задание 3. Создание задания посредством Enterprise Manager.

1. Установите средствами Enterprise Manager соединение с учебным экземпляром SQL Server.

2. В контейнере SQL Server Agent щелкните значок Jobs и выберите команду New Job.

3. В поле имя задайте имя задания – Backup Base собств имя Tlog.

4. Создайте этап задания с именем Backup Tlog Step

5. В поле Command введите оператор Transact-SQL BACKUP LOG JobBD_собст_имя TO DISK='C:\DB\444\JobDB_имя.trn'.

6. Щелкните кнопку Parse для проверки синтаксиса команды. Если отсутствуют ошибки, перейдите к следующему шагу.

7. Создайте расписание выполнения задания: ежедневно по рабочим дням в 20:00.

8. Задайте в качестве оператор собственное имя.

9. Просмотрите результаты создания задания.

10. Запустите задание, просмотрите результаты работы.

Задание 4. Создание задания посредством Enterprise Manager.

1. Установите средствами Enterprise Manager соединение с учебным экземпляром SQL Server.

2. Выберите контейнер Management.

3. Создайте план обслуживания, обеспечивающий проверку целостности собственной БД и оптимизацию размера БД. Задайте в качестве имени плана - собственное имя.

4. Установите время запуска плана, обеспечивающего начало его выполнение в течение 3 минут, уставновите место размещщения журнала выполнения данного плана c:\db\444\.

5. Проверьте выполнение указанного плана в списке заданий, какие операции выполняеются?

6. Проверьте результаты выполнения собственного плана. Если есть ошибки, то какова их причина.

7. Какие возможные операции могут быть включены в план обслуживания БД?

## 3. Методические рекомендации (указания) к лабораторным занятиям

### Установка и конфигурирование Windows Server 2003. Роли сервера и их назначение

Цель работы: приобретение студентами практических навыков установки операционной системы Microsoft Windows Server 2003. Ознакомиться и изучить роли серверов и их назначение.

Общие сведения

Разработанная для предприятий среднего и большого бизнеса операционная система Windows Server 2003 Enterprise Edition позволяет развертывать легкодоступные и масштабируемые приложения на стандартном оборудовании. В результате пользователь получает высокопродуктивную инфраструктуру, оптимизированную для запуска ответственных бизнесприложений и служб. Общими приме-рами приложений, которые могут выполняться в ОС Windows Server 2003 Enterprise Edition, являются приложения для работы в сети и обмена сообщениями, системы инвентаризации и клиентских служб, системы баз данных, узлы электронной коммерции, файловые серверы и серверы печати. Данная операционная система обеспечивает высокую надежность, производительность и экономическую эффективность.

Все операционные системы семейства Windows Server 2003, включая Windows Server 2003 Enterprise Edition, являются многозадачными операционны-ми системами, способными централизовано или распределено управлять различ-ными наборами ролей, в зависимости от потребностей пользователей.

В операционных системах семейства Windows Server 2003 доступны следующие роли сервера:

- файловый сервер;
- сервер печати;
- сервер приложений;
- почтовый сервер;
- сервер терминалов;
- сервер удаленного доступа и VPN-сервера;
- контроллер домена;
- DNS-сервер (система доменных имен);
- DHCP-сервер (сервер протокола динамической настройки узлов);
- сервер потоков мультимедиа;
- WINS-сервер.

Файловый сервер предназначен для предоставления доступа к файлам и управления ими. Если планируется использовать дисковое пространство данного компьютера для хранения, управления и общего доступа к данным в виде файлов и доступных в сети приложений, то данный компьютер следует настроить как файловый сервер.

Настройка роли файлового сервера позволяет отслеживать и ограничивать дисковое пространство, доступное отдельным пользователям. Также можно задать, что необходимо регистрировать в журнале - превышение пользователем заданного дискового пространства или превышение пользователем указанного порога предупреждения (то есть отметки, при прохождении которой пользователь приближается к заданному для него или нее пределу использования дискового пространства). Для быстрого и безопасного поиска информации (как локального, так и в сети) можно использовать Службу индексирования. Настройка роли файлового сервера позволяет производить поиск в файлах различных форматов и на разных языках либо при помощи команды "Найти" в меню Пуск, либо при помощи страниц HTML, отображаемых обозревателем.

Сервер печати предоставляет доступ к принтерам и управляет им. Если планируется удаленное управление принтерами, управление принтерами при помощи Инструментария управления Windows (WMI) или печать с сервера или компьютера клиента на сервер печати, используя URL-адрес, то данный компьютер следует настроить как сервер печати.

После того как задана роль сервера печати, появляется возможность использования обозревателя для управления принтерами. Можно приостанавливать, возобновлять и удалять задания на

печать, а также просматривать состояние принтера и заданий на печать. Также можно использовать созданный корпорацией Майкрософт инструментарий управления Windows (WMI), являющийся интерфейсом управления API, что позволяет отслеживать и контролировать все компоненты системы, как локальные, так и удаленные. Служба доступа к принтерам WMI позволяет управлять серверами печати, устройствами печати и прочими связанными с печатью объектами из командной строки. Служба доступа к принтерам WMI допускает использование сценариев Visual Basic (VB) для администрирования принтеров. Настройка роли серверами печати позволяет осуществлять печать с клиентов Windows XP на сервере печати под управлением Windows Server 2003, используя URL-адрес. Можно подключаться к общим принтерам сети путем установки их одним щелчком через Интернет. Имеется возможность установки драйверов с веб-узла

Сервер приложений представляет собой базовую технологию, обеспечивающую инфраструктуру ключа и службы, для приложений, находящихся в системе. Обычно серверы приложений содержат перечисленные ниже службы.

1. группировка ресурсов в пул (например, группировка в пул соединения базы данных и объекта);
2. управление распределенными транзакциями;
3. асинхронная связь программ, в основном при помощи очереди сообщений;
4. модель оперативной активации объекта;
5. интерфейсы автоматических веб-служб XML для доступа к рабочим объектам;
6. службы перемещения при сбое и определения работоспособности приложений;
7. интегрированная безопасность.

Операционные системы семейства Windows Server 2003 включают сервер приложений, содержащий все эти и другие службы для разработки, развертывания и рабочего цикла управления веб-службами XML, веб-приложениями и распределенными приложениями.

При настройке сервера приложений производится установка информационных служб Интернета (IIS) и других необязательных технологий и служб, таких как COM+ и ASP.NET. Работая вместе с информационными службами Интернета, операционные системы семейства Windows Server 2003 обеспечивают интегрированные, надежные, масштабируемые, безопасные и управляемые возможности веб-серверов для использования как в интрасети и в Интернете, так и во внешних сетях. IIS является средством создания усиленной платформы соединений для динамических сетевых приложений

Почтовый сервер. Для предоставления пользователям служб электронной почты могут быть использованы Протокол Post-Office Protocol, версия 3 (POP3) и Протокол SMTP, являющиеся входящими в состав семейства операционных систем Windows Server 2003 компонентами. Служба POP3 использует стандартный протокол POP3 для извлечения почты и может быть использована вместе со службой SMTP для передачи почты. Если планируется поддерживать клиентские соединения с данным сервером POP3 и получать электронную почту на локаль-ный компьютер при помощи почтового клиента, поддерживающего POP3, то сле-дует настроить данный сервер как почтовый сервер.

После того как задана роль почтового сервера, появляется возможность выполнять следующие действия:

1. использовать службу POP3 для хранения учетных записей электронной почты и управления ими на почтовом сервере;
2. включить доступ пользователя к почтовому серверу, чтобы он мог получать электронную почту со своего локального компьютера при помощи поддерживающего протокол POP3 клиента электронной почты (например, Microsoft Outlook).

При помощи сервера терминалов можно предоставить одну точку установки, позволяющую нескольким пользователям получить доступ к любому компьютеру под управлением операционной системы Windows Server 2003. Пользователи могут запускать программы, сохранять файлы и использовать ресурсы сети с удаленного компьютера так, как если бы эти ресурсы были установлены на их компьютере.

После того как задана роль сервера терминалов, появляется возможность выполнять следующие действия:

1. проверять параметры расширенной настройки безопасности Internet Explorer;

2. централизованно разворачивать программы на одном компьютере;

3. обеспечить использование клиентами одной и той же версии программы.

Сервер удаленного доступа и VPN-сервера. Маршрутизация и удаленный доступ обеспечивают полнофункциональный программный маршрутизатор, удаленное соединение и соединение виртуальных частных сетей (VPN) для удаленных компьютеров. Также предлагаются службы маршрутизатора для локальной сети (LAN) и глобальной сети (WAN). Такой сервер позволяет удаленным или мобильным сотрудникам получить доступ к корпоративным сетям при подключении напрямую, либо через службы удаленного соединения, либо через Интернет при помощи VPN-соединения. Если планируется подключать удаленных сотрудников к офисной сети, сервер следует настроить как сервер удаленного доступа или VPN-сервер. Соединения удаленного доступа включают все обычно доступные пользователям локальной сети службы, включая службы совместного использования файлов и принтеров, доступ к веб-серверу и службу сообщений.

После того как задана роль сервера удаленного доступа или VPN-сервера, появляется возможность выполнять следующие действия:

1. контролировать время и место доступа пользователей в сеть;

2. использовать службы преобразования сетевых адресов (NAT) для компьютеров в сети;

3. создавать собственные сетевые решения, используя интерфейсы программирования приложений (API).

Контроллеры домена хранят данные каталога и управляют взаимодействием между пользователями и доменом, а именно: процессом входа в домен, проверкой подлинности и поиском в каталоге. Если планируется позволить службе каталогов Active Directory управлять пользователями и компьютерами, следует настроить данный сервер как контроллер домена.

После того как задана роль контроллера домена, появляется возможность выполнять следующие действия:

1. Сохранять данные каталога и делать их доступными для пользователей сети и администраторов. Служба каталога Active Directory, хранящая сведения об объектах сети, предоставляет возможность пользователям и администраторам легко находить эти данные, обеспечивая логическую иерархическую организацию данных. Служба каталога Active Directory хранит сведения об объектах сети, например, имена, пароли, номера телефонов и тому подобные сведения и предоставляет возможность пользователям и администраторам той же сети, прошедшим проверку, получать доступ к этим сведениям.

2. Создавать дополнительные контроллеры домена в существующем домене для повышения доступности и надежности сетевых служб.

3. Повысить производительность сети между сайтами путем размещения контроллера домена на каждом сайте. Размещение контроллера домена в каждом сайте позволяет выполнять процесс входа в сеть внутри сайта без использования медленных подключений между сайтами.

4. DNS представляет собой службу разрешения имен TCP/IP, используемую в Интернете. Служба DNS позволяет компьютерам клиентов в сети регист-рировать и сопоставлять понятные имена DNS. Если планируется сделать ресурсы сети доступными в Интернете, сервер следует настроить как DNS-сервер.

5. После того как задана роль сервера DNS, появляется возможность вы-полнять следующие действия:

6. Поддерживать записи в распределенной базе данных DNS и использовать эти записи для обработки DNS-запросов, созданных DNS-клиентами, таких как запросы имен веб-сайтов или компьютеров в сети или в Интернете.

7. Именовать и располагать сетевые ресурсы, используя понятные имена.

8. Контролировать разрешение имен для каждого сегмента сети и реплици-ровать изменения или внутри всей сети, или глобально в Интернете.

9. Уменьшить администрирование DNS за счет динамического обновления DNS-сведений.

DHCP-сервер. Протокол DHCP (Dynamic Host Configuration Protocol) - это стандарт протокола IP, разработанный для уменьшения сложности администри-рования настроек адресов, используя компьютер сервера для централизованного управления IP-адресами и другими связанными подробностями настройки, ис-пользуемыми в сети. Если планируется выполнять распределение адресов многоадресной рассылки и получать клиентские IP-адреса и связанные динамически параметры конфигурации, следует настроить сервер как DHCP-сервер.

После того как задана роль сервера DHCP, появляется возможность выпол-нять следующие действия.

1. Централизованно управлять IP-адресами и связанной с ними информацией.

2. Использовать DHCP для предотвращения конфликтов адресов, вызываемых использованием ранее назначенного IP-адреса при настройке нового компь-ютера в сети.

3. Настраивать серверы таким образом, чтобы поддерживать полный диапазон дополнительных значений настройки при назначении аренды адреса. Это позволит значительно снизить время, затрачиваемое на настройку и перенастрой-ку компьютеров в сети.

4. Использовать при частом обновлении конфигурации клиентов (напри-мер, для пользователей с переносными компьютерами, часто меняющими распо-ложение) процесс обновления аренды DHCP с целью гарантировать эффективное и автоматическое внесение нужных изменений клиентами за счет обращения не-посредственно к DHCP-серверам.

Серверы потоков мультимедиа позволяют организации использовать служ-бы Windows Media. С помощью служб Windows Media можно управлять содер-жимым этих служб, включая потоковые аудио- и видеоданные, архивировать его и доставлять через интрасеть или Интернет. Если планируется использовать циф-ровое мультимедиа в режиме реального времени через удаленное Интернет соединение или через локальную сеть, следует настроить сервер как сервер потоков мультимедиа.

После того как задана роль сервера потокового мультимедиа, появляется возможность выполнять следующие действия:

1. Транслировать цифровое видео в режиме реального времени посредст-вом сетей с низкой пропускной способностью, при удаленном соединении через Интернет с высокой пропускной способностью, а также через локальную сеть.

2. Транслировать потоковое цифровое аудио клиентам и другим серверам через Интернет или Интранет.

Серверы Windows Internet Name Service (WINS) отображают IP-адреса в NetBIOS имена компьютеров и NetBIOS-имена компьютеров обратно в IP-адреса. Используя серверы WINS в организации, можно осуществлять поиск ресурсов по имени компьютера, которое проще запомнить, вместо его IP-адреса. Если плани-руется отображать NetBIOS-имена в IP-адреса или централизованно управлять базой данных, сопоставляющей имена и адреса, следует настроить сервер как WINS-сервер.

После того как задана роль сервера WINS, появляется возможность выпол-нять следующие действия:

1. Уменьшить широковещательный трафик в подсетях, связанный с NetBIOS, разрешением клиентам, запрашивающим WINS-серверы, непосредст-венно искать удаленные системы.

2. Поддерживать клиентов, использующих ранние версии Windows и NetBIOS, в сети. Этим типам клиентов разрешается просматривать списки уда-ленных доменов Windows без необходимости наличия локальных контроллеров доменов в каждой подсети.

3. Поддерживать DNS-клиентов. Этим клиентам позволено искать ресурсы NetBIOS, если внедрено объединение просмотра WINS.

Для установки Windows Server 2003 на сервер необходимо выполнить ряд ниже описанных процедур.

Запуск установки.

Установку можно запустить, загрузив компьютер с установочного компакт-диска или запустить из существующей операционной системы Windows. В любом случае программа установки запускается автоматически.

Такой способ установки Windows Server 2003 наиболее простой и подразумевает прохождение всех инсталляционных окон в "ручном" режиме.

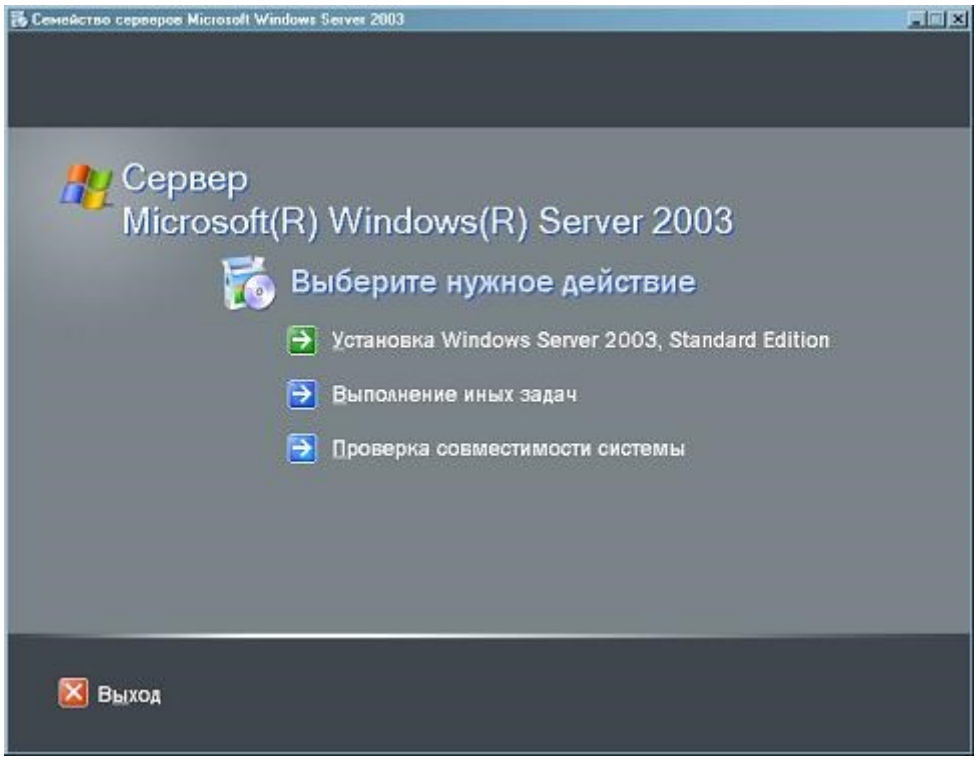
Если вам требуется установить большое количество серверов, то вы можете автоматизировать процесс установки, создав файлы ответов. Так же можно воспользоваться утилитой SysPrep для клонирования уже установленной системы Windows или использовать службу Remote Installation Services (RIS) для установки Windows через сеть.

Чтобы запустить установку Windows Server 2003 с компакт-диска, выполните следующее:

- Установите компакт-диск в дисковод.
- Выполните одно из следующих действий:
  - На компьютере с любой версией системы Windows, отличной от Windows 3.x, дождитесь отображения диалогового окна программы установки.
  - На компьютере с системой Windows 3.x воспользуйтесь диспетчером файлов, чтобы перейти в каталог I386 на компакт-диске, а затем дважды щелкните файл winnt.exe.
- Следуйте инструкциям по установке на экране.

При запуске программы установки на компьютере с Windows 3.x или MS-DOS для повышения эффективности работы следует воспользоваться программой кэширования дисков. В противном случае процесс установки (запущенный с помощью команды winnt.exe) может занять длительное время. Для включения кэширования диска на компьютере с Windows 3.x или MS-DOS можно использовать программу smartdrv.exe.

В диалоговом окне программы установки нажмите кнопку Install Windows Server 2003 (Установить Windows Server 2003).




Чтобы установить Windows через сеть, запустите программу winnt32.exe с сетевого диска, содержащего файлы установки Windows.

Процесс установки.

Процесс установки Windows Server 2003 аналогичен процессу установки Windows XP Professional и состоит из трех этапов:

• Выполнение программы установки позволяет создать раздел на диске, выбрать файловую систему и выполнить предварительное копирование файлов на жесткий диск, необходимых для установки Windows.

• Мастер установки соберет сведения о вас и вашем компьютере, настроит модемное и сетевое подключение, а так же поможет сделать ряд других настроек.

• Завершение установки подразумевает копирование всех необходимых файлов, настройку операционной системы, сохранение параметров.

На каждом из этапов выводятся запросы на ввод данных.

Программа установки.

Программа установки выполняется в несколько этапов:

1. В окне Welcome to Windows Setup выберите вариант New Installation (Advanced), чтобы начать инсталляцию Windows с нуля.

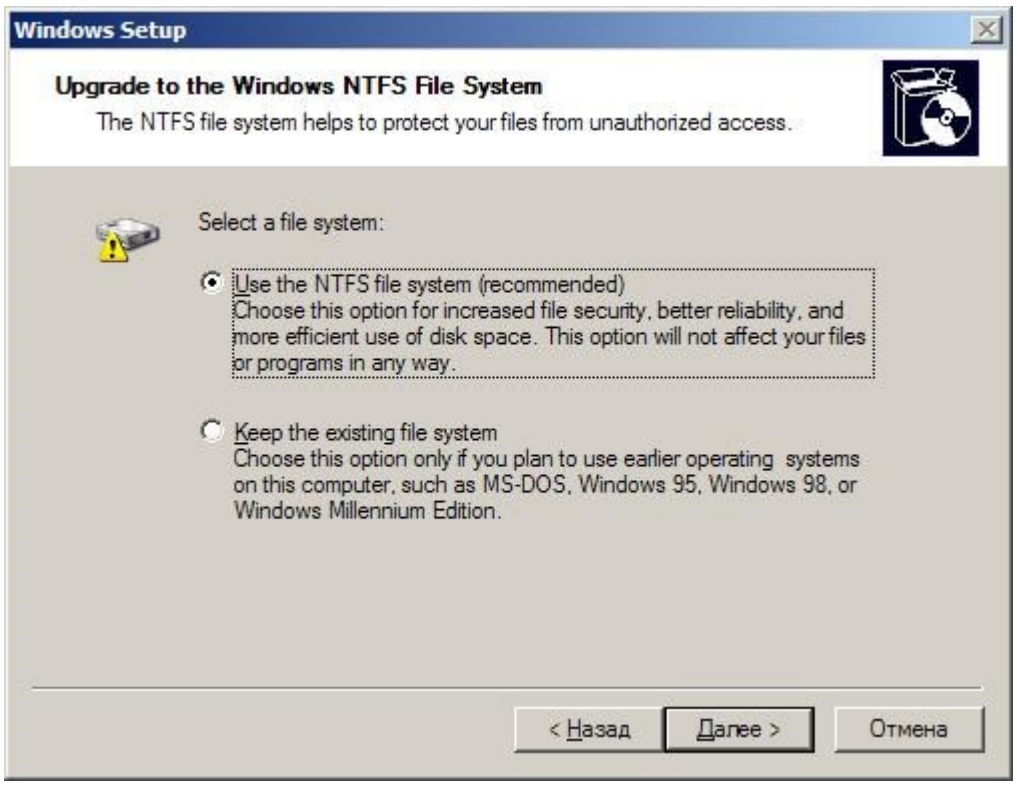

2. Прочитайте лицензионное соглашение, выберите вариант I accept this agreement (Я принимаю условия данного соглашения) и нажмите кнопку Далее (Next).

3. Введите код программного продукта, указанного на упаковке компакт-диска и нажмите кнопку Далее (Next).

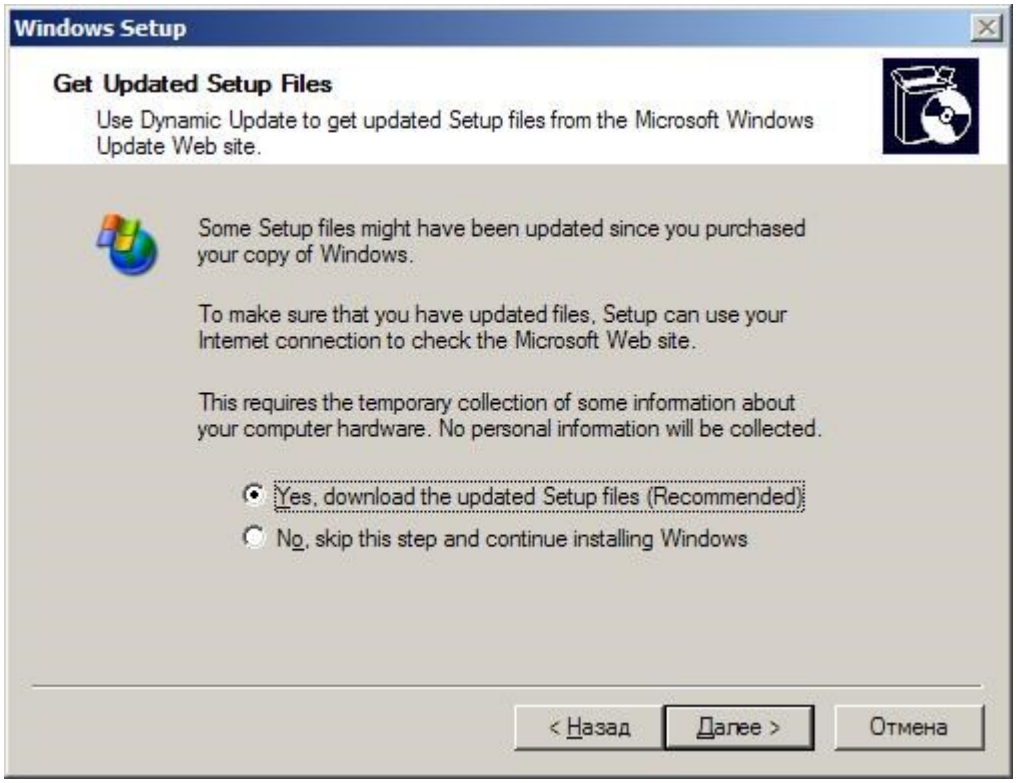
4. В окне Setup Options выберите основной язык из раскрывающегося списка. Нажав кнопку Advanced Options вы можете указать раздел жесткого диска, для установки Windows. Затем нажмите кнопку Далее (Next).



5. Укажите файловую систему, которую предполагаете использовать. Для полноценной работы сервера рекомендуется использование файловой системы NTFS, для этого выберите вариант Use the NTFS file system. Второй вариант Keep the existing file system позволит сохранить существующую файловую систему. Затем нажмите кнопку Далее (Next).




6. В окне Get Update Setup Files (Получение обновленных данных установки) выберите вариант Yes, download the updated Setup files, если хотите получить обновления немедленно. Для этого программа установки подсоединится к Интернету и загрузит все необходимые файлы. Чтобы пропустить этот шаг, установите переключатель в положение No, skip this step and continue installing Windows. Затем нажмите кнопку Далее (Next).



7. Программа установки перезагрузит компьютер в текстовую часть и продолжит установку.
8. На следующем этапе производится загрузка ядра Windows Server 2003, необходимых драйверов и самой программы установки. В самом начале загрузки программа установки предлагает установить дополнительные драйверы. Для этого нужно нажать клавишу F6. Программа установки попросит вставить в дисковод дискету с драйверами когда будет происходить загрузка драйверов.
9. После появления первого окна программы установки нажмите клавишу Enter, чтобы начать установку.
Для выхода из программы установки на любом ее этапе нажмите клавишу F3.
10. Прочитайте лицензионное соглашение. Нажмите F8, чтобы принять его условия (если соответствующее окно появится).
11. Программа установки отображает все существующие разделы и свободное пространство на всех доступных дисках в системе. При помощи клавиш со стрелками вверх и вниз вы можете выбрать раздел, на который будет установлена Windows Server 2003. Вы также можете создавать (клавиша C) и удалять (клавиша D) разделы. Чтобы подтвердить удаление, нажмите клавишу L. При удалении системного раздела необходимо еще одно подтверждение. Это окно появится, если установлен флажок I want to choose the installation partition during setup на шаге 4 данного раздела, или если вы загрузились с CD-ROM.
Программа установки не позволит удалить системный раздел при многовариантной загрузке или установке с жесткого диска или по локальной сети, т. к. здесь содержаться файлы, необходимые для запуска и работы программы установки и ядра Windows Server 2003.
Программа установки не позволит удалить раздел, на котором находятся файлы установки (постоянные или временные).
Можно использовать только часть доступного дискового пространства, указав ее объем. Для корректной работы Windows Server 2003 необходимо создать раздел объемом не менее 2,5 Гбайт (2500 Мбайт).
12. При использовании уже существующего раздела (не созданного на предыдущем шаге) программа установки предлагает конвертировать его в NTFS или оставить файловую систему без изменений.
При использовании нового неформатированного раздела программа установки предлагает отформатировать его под NTFS или FAT. При выборе FAT, если размер раздела менее 2048 Мб, будет использована FAT16, если больше - FAT32.
Программа установки осуществляет только полное форматирование раздела. Это может занять много времени.

Если вы планируете использовать мультизагрузку, с применением ОС Windows 9x, Me, не форматируйте диск C: в NTFS. Можно создать новый раздел для установки в него Windows Server 2003 и отформатировать этот раздел в NTFS.

Преобразовать раздел из формата FAT в формат NTFS можно позже, выполнив в командной строке утилиту Convert. Обратное преобразование (из NTFS в FAT) в Windows Server 2003 не предусмотрено.
13. После выбора раздела и, возможно, его форматирования программа установки осуществляет быструю проверку диска на наличие ошибок. При этом проверяются наиболее критические структуры диска.
14. Программа установки формирует каталог Windows Server 2003 (по умолчанию - Windows) и копирует в него необходимые файлы.
После копирования файлов загрузочная область системного диска модифицируется, инициализируется системный реестр, настраивается ядро Windows. После этого производится перезагрузка компьютера и переход к следующей фазе установки.

После перезагрузки не забудьте удалить все диски из приводов, в том числе и установочный CD-ROM.
Мастер установки Windows.

После перезагрузки запускается сконфигурированное ядро Windows Server 2003 с необходимым набором драйверов. После этого запускается графическая часть (Мастер установки Windows).

Используя довольно большую встроенную базу устройств, мастер установки осуществляет поиск и настройку устройств, поддерживающих технологию Plug and Play (PnP-устройств). На данном этапе можно быть уверенным, что будут обнаружены и установлены все устройства, упоминаемые в CL.

- Мастер установки предлагает выбрать региональные установки для настройки Windows Server 2003. К таким установкам относятся:
  - набор языков, поддерживаемых системой;
  - системный язык;
  - язык по умолчанию для пользователя;
  - настройки языка по умолчанию;
  - раскладки клавиатуры.

- Вы можете оставить настройки установленные по умолчанию, если они верны для вашего языка и региона, затем щелкните кнопку Далее. Для изменения параметров языковой настройки необходимо щелкнуть кнопку Настроить (изменить все эти параметры можно и после установки Windows).

Будьте внимательны при установке раскладки клавиатуры по умолчанию! Именно она используется в окне входа в Windows. Большинство пользователей не обращает внимания на индикатор раскладки при вводе пароля, что приводит к невозможности входа в Windows и/или блокировке учетной записи.

Все параметры настройки языков и стандартов начнут действовать со следующего шага мастера установки. Это относится, в том числе, и к способу переключения раскладок клавиатуры.

- Затем мастер установки переходит к информационной странице, в которой необходимо указать имя пользователя, на которого зарегистрирована копия Windows Server 2003. Можно указать название вашей организации, хотя это не обязательно. Данные, введенные на этом шаге, будут использоваться приложениями для формирования сведений об авторе документа.
- Далее мастер переходит к вводу ключа продукта, если он еще не введен. Вы должны ввести 25-значный ключ, который вы найдете на упаковке компакт-диска Windows Server 2003. Ключ может использоваться только для установки одной копии Windows. Для установки Windows Server 2003 на несколько компьютеров вы должны приобрести пакет лицензий и использовать ключ, полученный с этим пакетом.
- В следующем окне выберите режим работы лицензирования для сервера "на сервер" (Per Server) и "на рабочее место" (Per Seat). При выборе режима Per Server укажите, сколько клиентских лицензий для доступа к серверу (CAL) вы приобрели.
- На следующем шаге мастера установки вы должны ввести имя компьютера длиной не более 63 символов. Если нужна совместимость с клиентами Windows версии до Windows 2000 (пред-Windows), то максимальная длина имени компьютера не должна превышать 15 символов. Имя должно отличаться от имен остальных компьютеров, а также от имен рабочих групп и доменов в сети. Программа установки автоматически генерирует имя компьютера, исходя из названия организации, на которую зарегистрирована копия Windows, и некоторого случайного числа, гарантируя тем самым уникальность имени. Вы можете дать компьютеру более осмысленное имя или оставить предложенное по умолчанию.

При вводе имени компьютера, независимо от выбранного на клавиатуре регистра, имя отображается только прописными буквами.

Далее вы должны ввести пароль для учетной записи администратора. В русской версии Windows Server 2003 учетная запись администратора называется Администратор, в оригинальной американской версии - Administrator. Пароль учетной записи может иметь длину до 14 символов, хотя его можно оставить пустым, но это крайне не рекомендуется делать. Простым паролем или его отсутствием могут воспользоваться злоумышленники, подключившиеся через локальную сеть. Старайтесь всегда назначать для учетной записи администратора сложный пароль, состоящий из символов верхнего и нижнего регистров, цифр и спецсимволов. Рекомендуется использовать пароль

длинной не менее 8 символов, а также, на ряду с символами нижнего регистра, использовать хотя бы один символ верхнего регистра, одну цифру и один спецсимвол (например, f

- 4Wyz9c).
- Мастер установки переходит к окну настройки даты и времени. Проверьте правильность установки времени и даты. Перед корректировкой не забудьте выбрать правильный часовой пояс. Установите флажок Автоматический переход на летнее время и обратно, если это необходимо, затем щелкните кнопку Далее.

Если вы используете мультизагрузку, и в другой операционной системе используется автоматический переход на летнее/зимнее время, то во избежание повторного перехода, установите этот флажок только в одной из операционных систем

- Если в компьютере установлен модем, то далее мастер установки переходит к окну настройки параметров модемного соединения. Если страна (или регион), установленная по умолчанию, выбрана верно, в следующем поле введите код города. Установите правильный тип набора номера (в большинстве случаев это импульсный), затем щелкните кнопку Далее.
- Далее мастер установки переходит к настройке сетевых подключений и предлагает один из двух вариантов настройки сетевых параметров: типичные (Typical Settings) и особые (Custom). В первом случае программа установки использует параметры по умолчанию перечисленных выше компонентов для каждого сетевого адаптера. При выборе особых параметров вы можете изменить состав и/или конфигурацию сетевых компонентов вручную. В нашем варианте, для создания TCP/IP-сети, используются параметры, принятые по умолчанию (типичная установка), поэтому убедитесь, что выбрана именно типичная установка, и нажмите кнопку Далее.

Для каждого обнаруженного сетевого адаптера устанавливаются следующие компоненты:

- клиент для сетей Microsoft (Client for Microsoft Networks);
- служба совместного доступа к файлам и принтерам Microsoft (File and Printer Sharing for Microsoft Networks);
- протокол TCP/IP, настроенный на получение параметров по протоколу DHCP.

- Мастер установки переходит к окну выбора домена или рабочей группы. Вы должны указать, будет компьютер членом рабочей группы или членом домена. Также нужно будет ввести имя рабочей группы или домена.

Для подключения к одноранговой сети установите флажок Нет, этот компьютер не находится в сети, или подключен к сети без домена (No, this computer is not on a network, or is on a network without a domain) и укажите имя рабочей группы (обычно WORKGROUP).

Если вы хотите включить компьютер в сеть с выделенным сервером (при условии, что домен развернут), установите флажок Да, включить этот компьютер в домен (Yes, make this computer a member of the following domain), и укажите имя домена. После щелчка кнопки Далее программа установки запросит имя и пароль пользователя, имеющего право на создание учетной записи компьютера в домене. Сразу же после выполнения этого шага компьютер будет добавлен в домен. Если вы хотите создать новый домен, присоединитесь к рабочей группе или к существующему домену. Новый домен вы создадите позже.

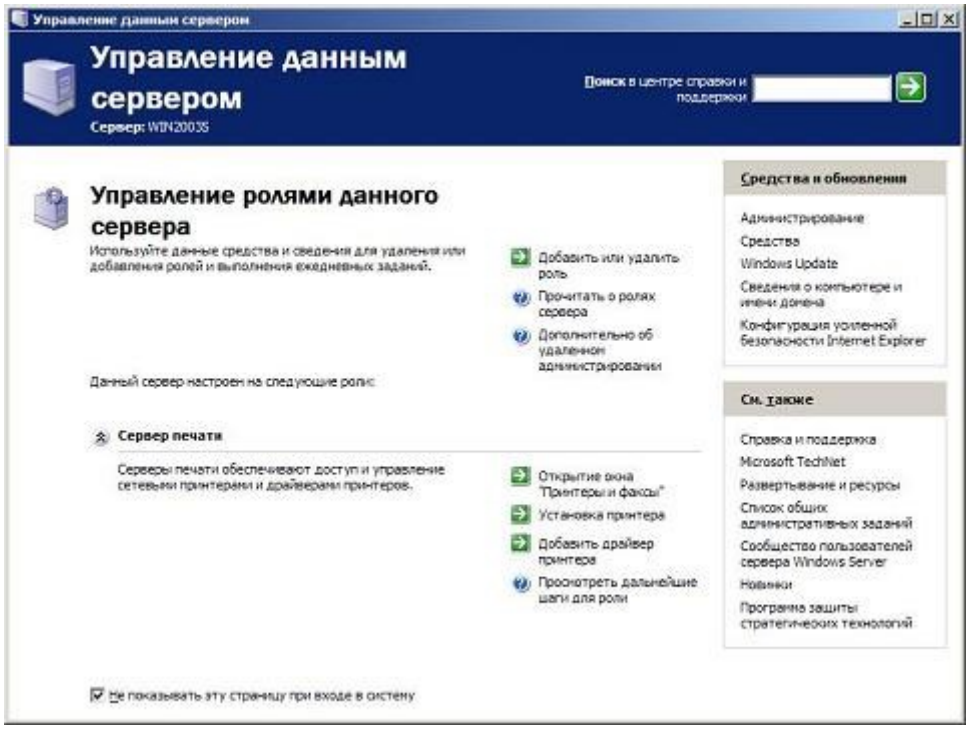
По окончании всех вышеуказанных настроек мастер установки начинает копировать необходимые файлы. Этот процесс может занять несколько минут.

Завершение установки.

Во время первого запуска Windows Server 2003 осуществляет настройку большинства Plug and Play устройств. После загрузки создаются ветви реестра, отвечающие за последнюю успешную и текущую конфигурации. Применяется стандартная локальная политика безопасности.

После загрузки Windows Server 2003 вы увидите стандартное окно входа, в котором необходимо ввести пароль администратора (его имя уже будет подставлено в поле Пользователь).

Сразу после первого входа в систему будет запущена утилита Управление данным сервером для настройки Windows Server 2003.




Она предназначена для быстрого запуска утилит, отвечающих за конфигурирование определенных служб. Чтобы данное окно не появлялось при каждом запуске Windows, установите флажок Не показывать эту страницу при входе в систему в нижней часть окна. Для дальнейшей настройки сервера вы всегда можете вызвать это окно из менюАдминистрирование.

Задание: выполнить вышеуказанные этапы установки  установки операционной системы Microsoft Windows Server 2003. Ознакомиться и изучить роли серверов и их назначение. Представить отчет по проделанной работе.

Контрольные вопросы:

1. Какие роли доступны серверу Windows Server 2003?
2. Какие службы обычно содержат серверы?
3. Что такое Windows Server 2003?
4. Укажите основные этапы установки Windows Server 2003

**Установка и настройка Active Directory**

Цель работы: приобретение студентами практических навыков установки и настройки Active Directory.

Общие сведения

Каталог представляет собой иерархическую структуру, которая хранит све-дения об объектах в сети. Служба каталогов, такая как Active Directory, обеспечи-вает возможность хранения данных каталога и доступа к этим данным сетевых пользователей и администраторов. Например, в Active Directory хранятся сведе-ния об учетных записях пользователей, такие как имена, пароли, номера телефо-нов и тому подобные, к которым могут получать доступ другие пользователи той же сети, прошедшие проверку.

Служба каталогов - одна из наиболее важных составных частей развитой компьютерной системы. Пользователи и администраторы зачастую не знают точ-ных имен нужных им объектов, которые им в данный момент требуются. Они мо-гут знать один или несколько их признаков или атрибутов (attributes) и могут по-слать запрос (query) к каталогу, получив в ответ список тех объектов, атрибуты которых совпадают с указанными в запросе. Служба каталогов позволяет найти любой объект по одному из его атрибутов.

Служба каталогов Active Directory может быть установлена на серверах, ра-ботающих под управлением операционных систем Microsoft Windows Server 2003, Standard Edition, Windows

Server 2003, Enterprise Edition и Windows Server 2003, Datacenter Edition. Она хранит сведения об объектах сети и упрощает поиск и ис-пользование этих сведений пользователям и администраторами. В Active Directory основой для логической, иерархической организации сведений каталога служит структурированное хранилище данных. Это хранилище данных, называемое так-же каталогом, содержит сведения об объектах Active Directory. В число этих объ-ектов обычно входят общие ресурсы, такие как серверы, тома, принтеры, а также учетные записи сетевых пользователей и компьютеров.

Служба каталогов позволяет обеспечивать защиту информации от вмеша-тельства посторонних лиц в рамках, установленных администратором системы. Группа безопасности интегрирована с Active Directory посредством проверки подлинности при входе в сеть и управления доступом к объектам в каталоге. В рамках одного входа в сеть администраторы могут управлять данными каталога и организацией через их сеть, а прошедшие проверку сетевые пользователи могут иметь доступ к ресурсам во всей сети. Администрирование, основанное на поли-тике, облегчает управление даже самой сложной сетью.

В состав службы Active Directory входят также следующие элементы:

Набор правил - схему, определяющую классы объектов и атрибуты, содер-жащиеся в каталоге, а также пределы и ограничения на экземпляры этих объек-тов, и формат их имен.

Глобальный каталог, содержащий сведения о каждом объекте в каталоге. Это позволяет пользователям и администраторам находить сведения каталога не-зависимо от того, в каком из доменов каталог в действительности содержатся эти данные.

Механизм запросов и индексации, позволяющий опубликовывать и нахо-дить объекты и их свойства сетевым пользователям или приложениям.

Службу репликации (тиражирования), распространяющую данные каталога по сети. Все контроллеры домена в домене участвуют в репликации и содержат полную копию всех сведений каталога для своего домена. Любое изменение дан-ных каталога реплицируется во все контроллеры домена в домене.

Определим основные понятия, используемые для описания Active Directory.

Область действия (scope) Active Directory достаточно обширна. Она может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети. Она может также охватывать не-сколько объединенных сетей.

Active Directory, как и любая другая служба каталогов, является, прежде всего, пространством имен. Пространство имен - это такая ограниченная область, в которой может быть распознано данное имя.

Распознавание имени заключается в его сопоставлении с некоторым объектом или объемом информации, которому это имя соответствует. Файловая система Windows образует пространство имен, в котором имя файла может быть поставлено в соответствие конкретному файлу. Active Directory образует пространство имен, в котором имя объекта в каталоге может быть поставлено в соответствие самому этому объекту.

Объект - это непустой, именованный набор атрибутов, обозначающий не-что конкретное, например, пользователя, принтер или приложение. Атрибуты со-держат информацию, однозначно описывающую данный объект. Атрибуты поль-зователя могут включать имя пользователя, его фамилию и адрес электронной почты.

Контейнер аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имен. Однако, в отличие от объекта, контейнер не обозначает ничего конкретного - он может содержать группу объектов или дру-гие контейнеры.

Термин дерево используется для описания иерархии объектов и контейне-ров. Как правило, конечными элементами дерева являются объекты. В узлах (точ-ках ветвления) дерева располагаются контейнеры. Дерево отражает взаимосвязь между объектами или указывает путь от одного объекта к другому. Простой ката-лог представляет собой контейнер. Компьютерная сеть или домен тоже являются контейнерами.

Домен - это единая область, в пределах которой обеспечивается безопас-ность данных в ком-

пьютерной сети под управлением ОС Windows Server 2003. Active Directory состоит из одного или нескольких доменов. Применительно к от-дельной рабочей станции доменом является сама рабочая станция. Границы одно-го домена могут охватывать более чем одно физическое устройство. Каждый до-мен может иметь свои правила защиты информации и правила взаимодействия с другими доменами. Если несколько доменов связаны друг с другом доверитель-ными отношениями и имеют единую логическую структуру, конфигурацию и глобальный каталог, то говорят о дереве доменов. Несколько доменных деревьев могут быть объединены в лес.

Дерево доменов (дерево) состоит из нескольких доменов, которые имеют общую логическую структуру и конфигурацию и образуют непрерывное про-странство имен. Домены в дереве связаны между собой доверительными отноше-ниями. Active Directory является множеством, которому принадлежат одно или несколько деревьев.

Лесом называется одно или несколько деревьев, которые не образуют не-прерывного пространства имен. Все деревья одного леса имеют общие логиче-скую структуру, конфигурацию и глобальный каталог. В отличие от дерева, лес может не иметь какого-то определенного имени.

Узлом называется такой элемент сети, который содержит серверы Active Directory. Узел обычно определяется как одна или несколько подсетей, поддержи-вающих протокол TCP/IP и характеризующихся хорошим качеством связи. "Хо-рошее" качество связи в данном случае подразумевает высокую надежность и скорость передачи данных. Определение узла как совокупности подсетей позво-ляет администратору быстро и без больших затрат настроить топологию доступа и репликации в Active Directory и полнее использовать достоинства физического расположения устройств в сети. Когда пользователь входит в систему, клиент Active Directory ищет серверы Active Directory, расположенные в узле пользовате-ля. Поскольку компьютеры, принадлежащие к одному узлу, в масштабах сети можно считать расположенными близко друг к другу, связь между ними должна быть быстрой, надежной и эффективной. Распознавание локального узла в момент входа в систему не составляет труда, так как рабочая станция пользователя уже знает, в какой из подсетей TCP/IP она находится, а подсети напрямую соответст-вуют узлам Active Directory.

В Windows Server 2003 Active Directory может быть интегрирована с DNS воедино. DNS представляет собой распределенное пространство имен, которое используется в Интернет и в котором именам отдельных компьютеров и служб ставятся в соответствие адреса, формируемые по правилам протокола TCP/IP. При создании контроллера домена, то есть сервера, управляющего работой Active Directory, мастер предлагает создать и настроить DNS-сервер. В этом случае за-пускается DNS-сервер и создается зона (контейнер, объединяющий несколько до-менов в структуру с общими разрешениями на управление), одноименная с доме-ном.

Контроллеры домена хранят данные и управляют взаимодействием пользо-вателей с доменом, включая процесс входа в домен, проверку подлинности и по-иск в каталогах. Чтобы предоставить сетевым пользователям и компьютерам службу каталогов Active Directory, нужно настроить данный сервер как контрол-лер домена.

Для настройки сервера в качестве контроллера домена необходимо устано-вить на данный сервер Active Directory. В мастере установки Active Directory дос-тупны четыре параметра: можно создать дополнительный контроллер домена в существующем домене, контроллер домена для нового дочернего домена, кон-троллер домена для нового доменного дерева или новый контроллер домена для нового леса. Рассмотрим создание контроллера домена для нового леса.

Операционная система Windows Server 2003 позволяет настроить данный сервер как контроллер домена. Для этого нам необходимо выполнить следующие действия: открыть оснастку "Управление данным сервером"; выбрать ссылку "Добавить или удалить роль"; на странице "Предварительные шаги" прочитать информацию о сетевых соединениях и подтвердить, что все они доступны; на странице "Параметры настройки" выбрать вариант "Особая конфигурация".

На экран будет выведена новая страница, представленная на рис. 20 - Роль сервера.

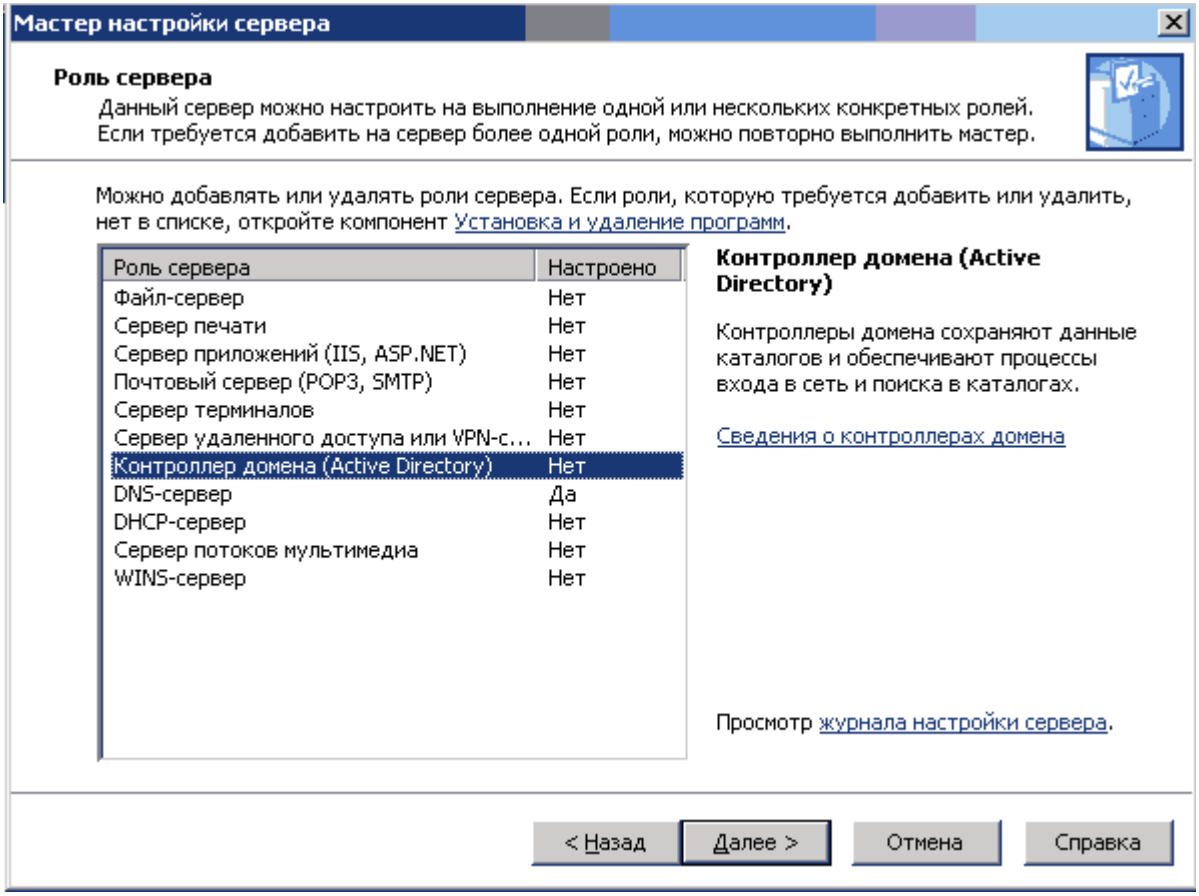



Рис. 20. Роль сервера

На этой странице мы выбираем из приведённого списка "Контроллер доме-на (Active Directory)" и нажимаем кнопку "Далее".

Появится страница "Сводка выбранных параметров" (рис. 21), в которой можно просмотреть и подтвердить выбранные параметры:

Для применения параметров, выбранных на странице "Сводка выбранных параметров", нажимаем кнопку "Далее".

Появится страница "Применение выбранных параметров", которая будет находиться на экране всё время до окончания установки и настройки Active Directory.

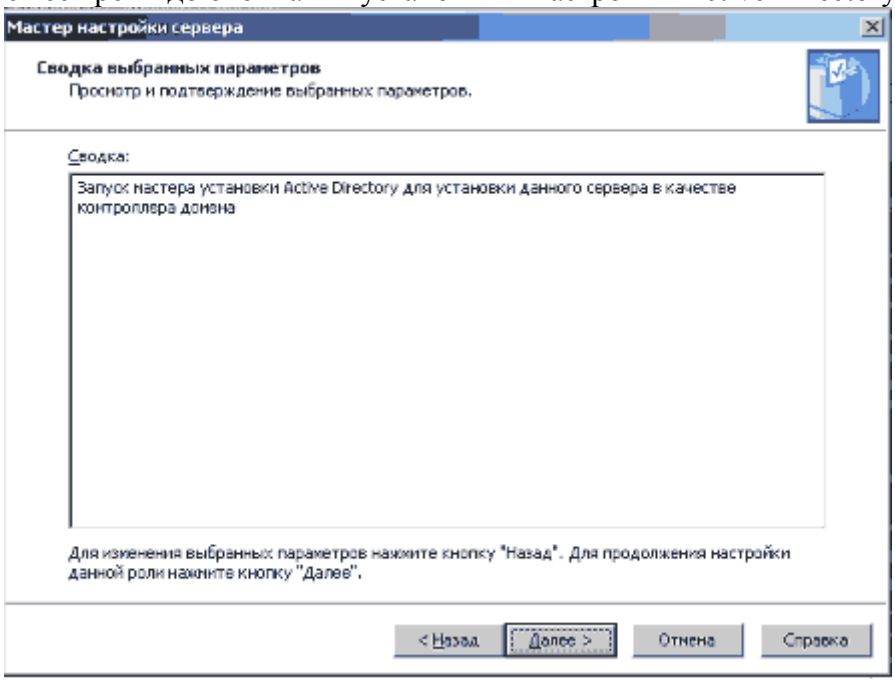



Рис. 21. Сводка выбранных параметров

Автоматически запустится мастер установки Active Directory.

Нажимаем кнопку "Далее" для продолжения. К этой странице можно вер-нуться из любого места мастера, пока не нажата кнопка "Готово" на последней странице.

Мастер установки выведет на экран страницу, представленную на рис. 23, "Совместимость операционных систем", в которой приводится информация о влиянии усовершенствованных параметров безопасности в Windows Server 2003 на совместимость с предыдущими версиями Windows.

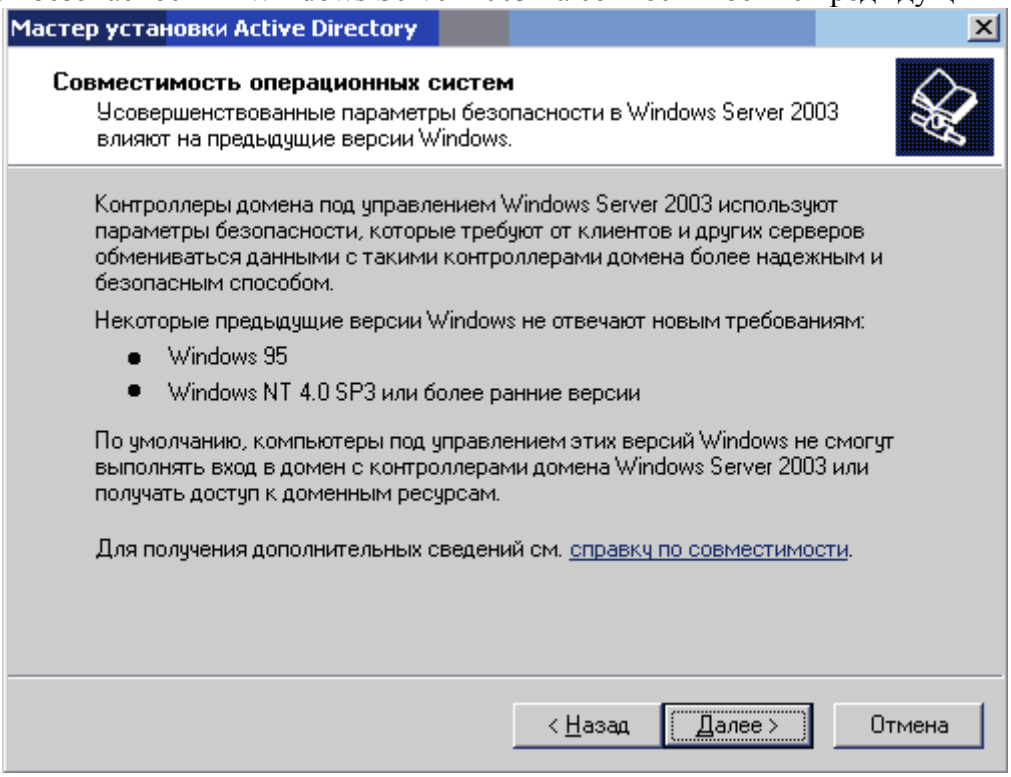



Рис. 23. Совместимость операционных систем

Прочитав сведения, приведённые на этой странице, нажимаем кнопку "Далее".

На странице "Тип контроллера домена" выбираем вариант "Контроллер домена в новом домене" (рис. 24).

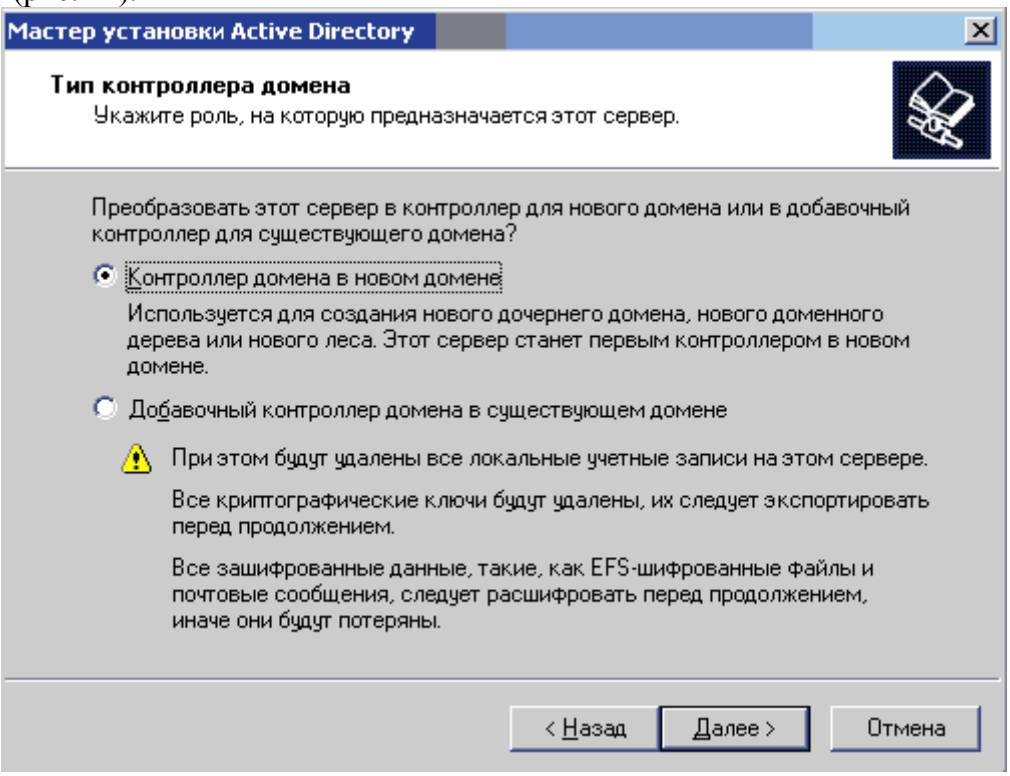



Рис. 24. Тип контролера домена

Для продолжения нажимаем кнопку "Далее".

На появившейся странице, представленной на рис. 25, "Создать новый домен" выбираем вариант "Новый домен в новом лесу".

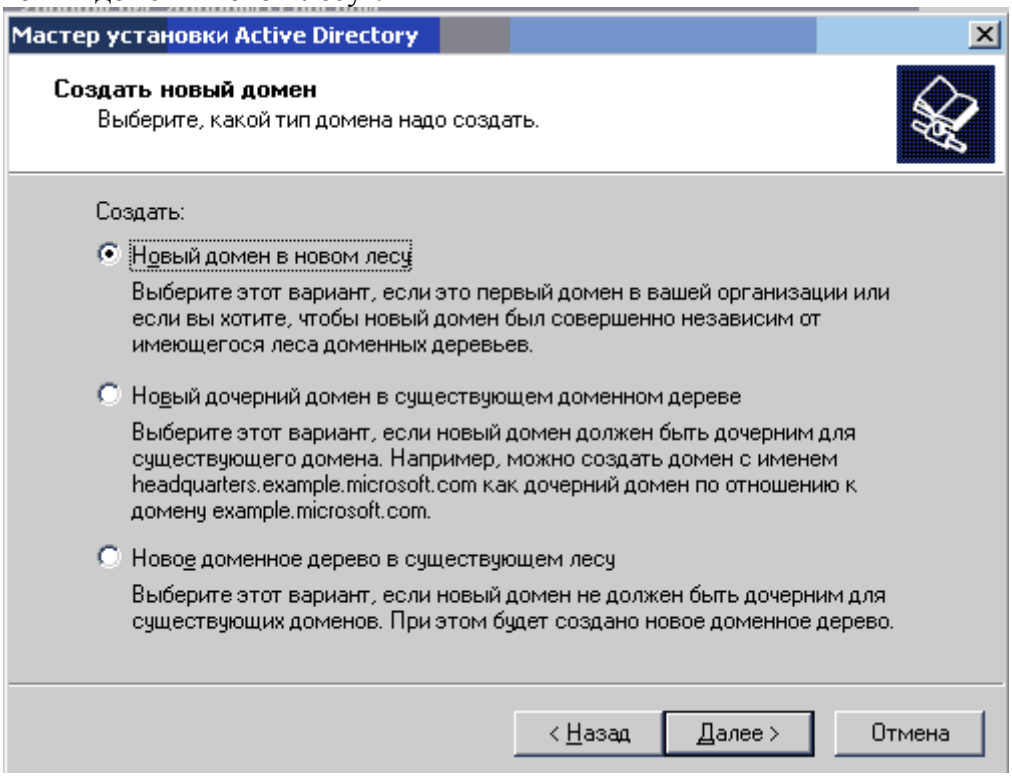



Рис. 24. Тип контролера домена

Для продолжения нажимаем кнопку "Далее". На странице "Новое имя домена" (рис. 26) вводим полное DNS-имя нового домена.

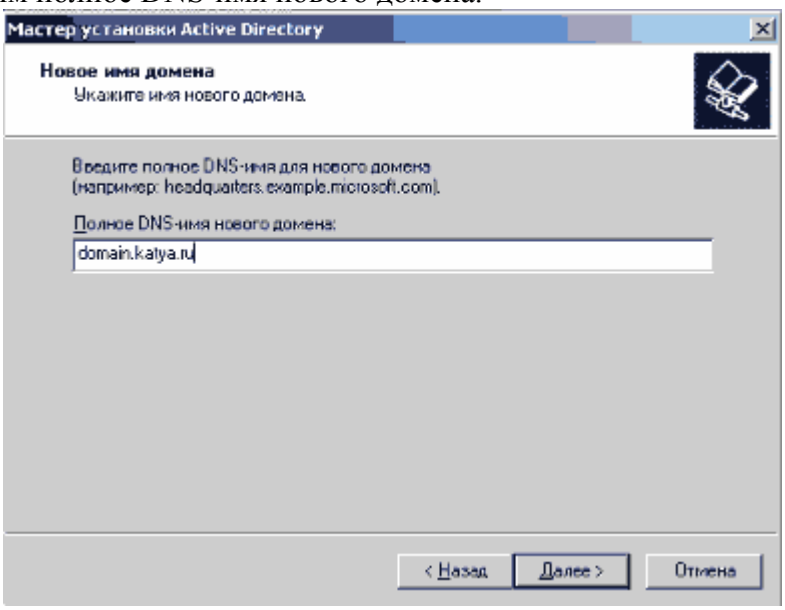



Рис. 26. Новое имя домена

Полное DNS-имя также называют полным доменным именем (FQDN). Домены Active Directory обозначаются с помощью DNS-имен и повторяют иерархическую структуру DNS. DNS-имена для леса Active Directory должны начинаться с зарегистрированного суффикса домена DNS, который зарезервирован организацией для использования в Интернете, например microsoft.com. Для продолжения нажимаем кнопку "Далее".

На странице NetBIOS-имя домена проверяем NetBIOS-имя, которое будет использоваться пользователями предыдущих версий Windows для идентификации домена (рис. 27).

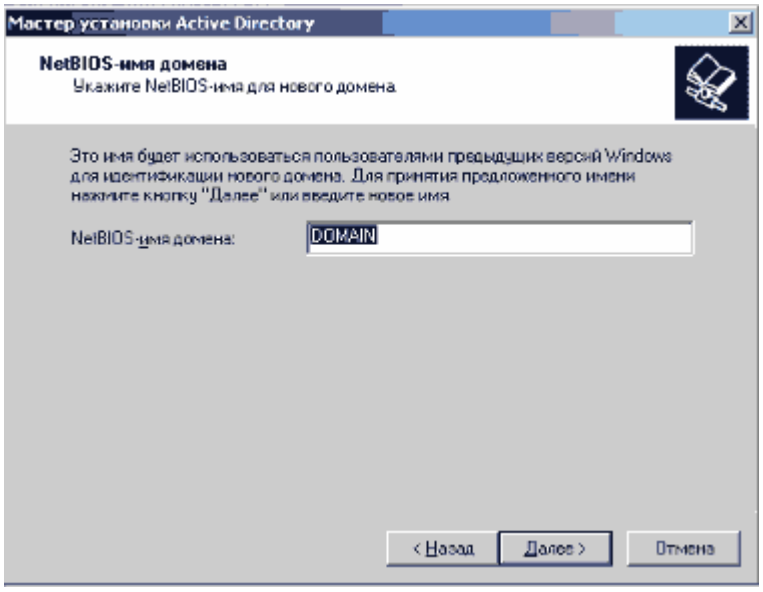



Рис. 27. NetBIOS-имя домена

Домены Active Directory обозначаются в соответствии со стандартами именования DNS, однако при создании доменов Active Directory необходимо задать также NetBIOS-имя. NetBIOS-имена по возможности должны совпадать с первой меткой DNS-имени домена. Если первая метка DNS-имени домена Active Directory отличается от его NetBIOS-имени, в качестве полного доменного имени используется DNS-имя, а не NetBIOS-имя. Например, если первая метка полного DNS-имени домена - child (child.microsoft.com), а NetBIOS-имя домена - sales, полным доменным именем будет child.microsoft.com. Для продолжения нажимаем кнопку "Далее". На странице "Папки базы данных и журналов", представленной на рис. 28, вводим расположение, в которое нужно установить папки базы данных и журналов (или нажимаем кнопку Обзор, чтобы указать расположение).

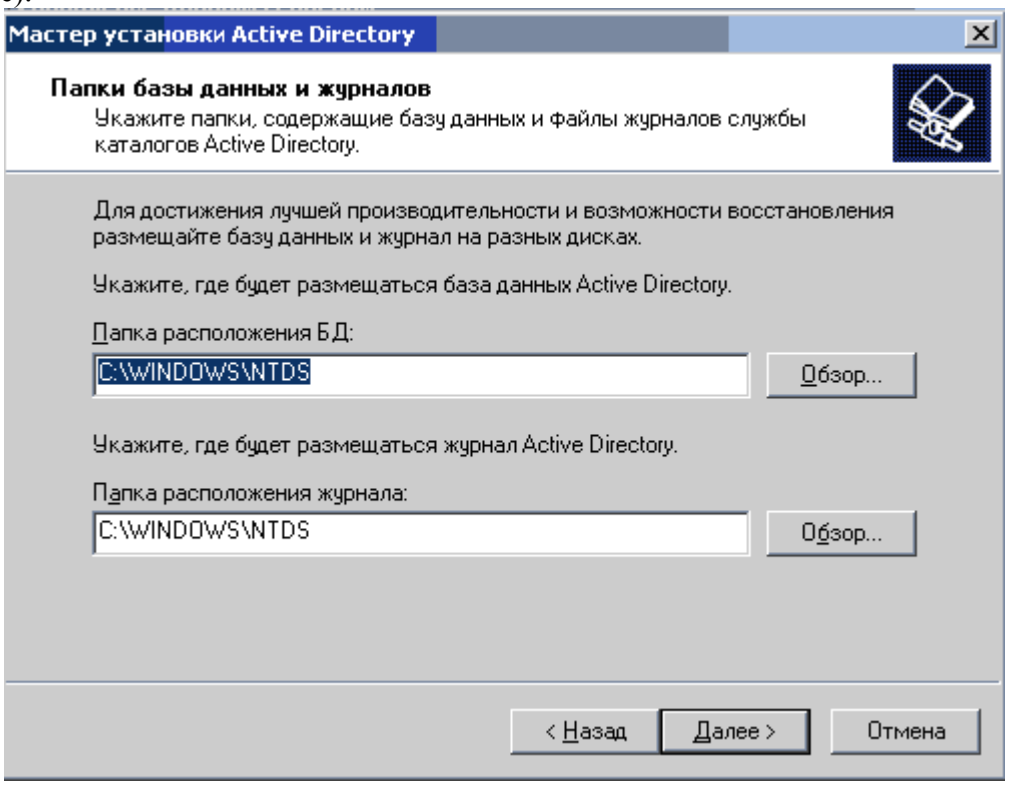



Рис. 28. Папки базы данных и журналов

При этом нужно убедиться, что на диске достаточно места для размещения базы данных каталога и файлов журналов, чтобы избежать проблем при установке или удалении Active Directory. Мастеру установки Active Directory необходимо 250 МБ дискового пространства для

установки базы данных Active Directory и 50 МБ для файлов журналов. Рекомендуется размещать данные файлы в разделе NTFS. Для продолжения нажимаем кнопку "Далее".

На странице "Общий доступ к системному тому" (рис. 29) указываем расположение, в которое следует установить папку Sysvol (или нажимаем кнопку Обзор, чтобы указать расположение).

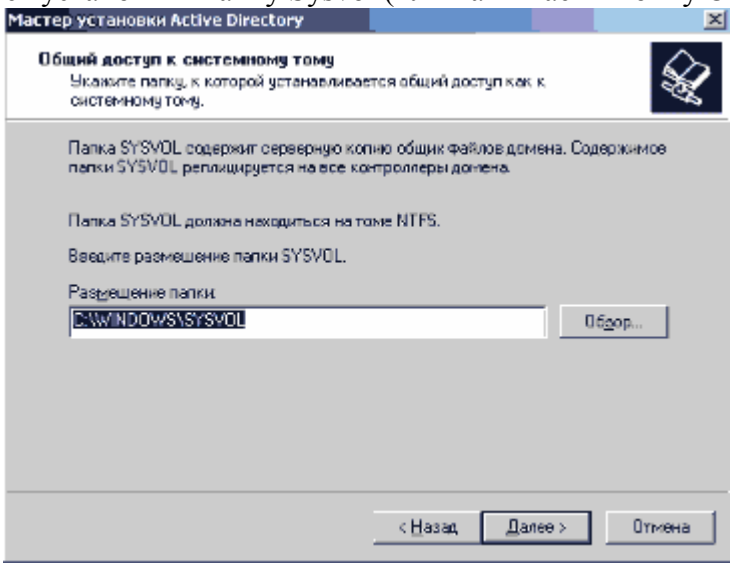



Рис. 29. Общий доступ к системному тому

Папка Sysvol должна находиться в томе NTFS, так как в ней находятся файлы, реплицируемые между контроллерами домена в домене или лесу. Эти файлы содержат сценарии, системные политики для Windows NT 4.0 и более ранних версий, общие папки NETLOGON и SYSVOL и параметры групповой политики. Для продолжения нажимаем кнопку "Далее". На странице "Диагностика регистрации DNS" (рис. 30) проверяем правильность установки параметров.

Если в окне "Результаты диагностики" отображается сообщение об ошибках диагностики, можно нажать кнопку "Справка" для получения дополнительных инструкций по устранению ошибки. Для продолжения нажимаем кнопку "Далее".

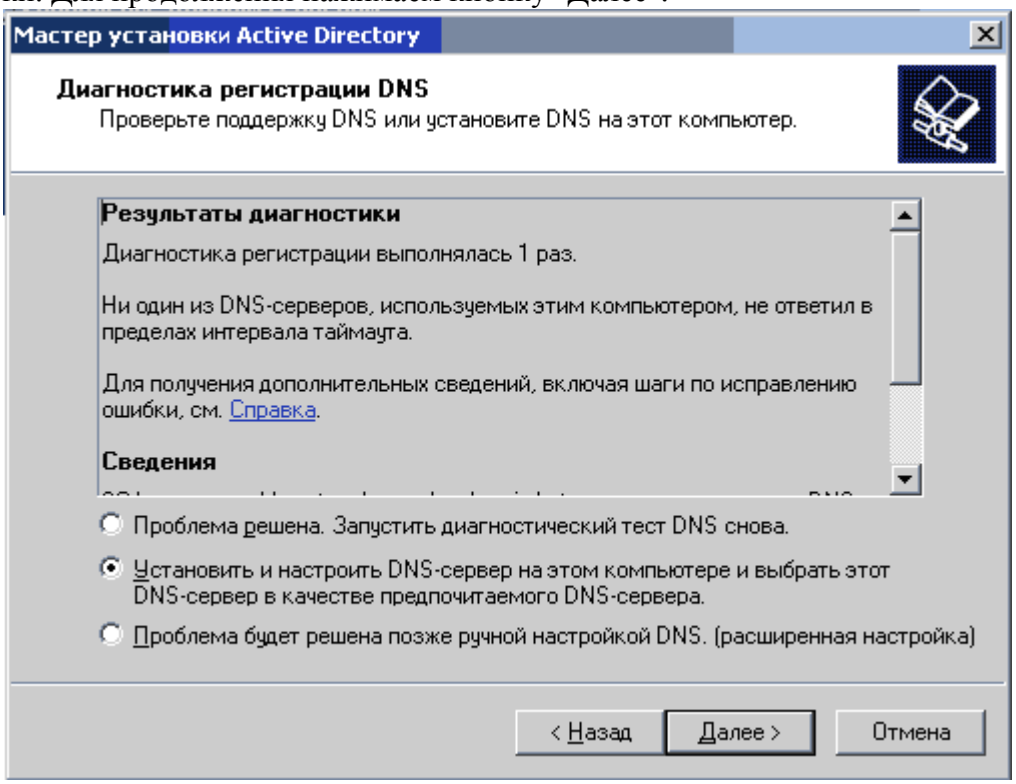



Рис. 30. Диагностика регистрации DNS

На странице "Разрешения" (рис. 31) выбираем требуемый уровень совместимости приложений с операционными системами пред-Windows 2000, Windows 2000 или Windows Server 2003.

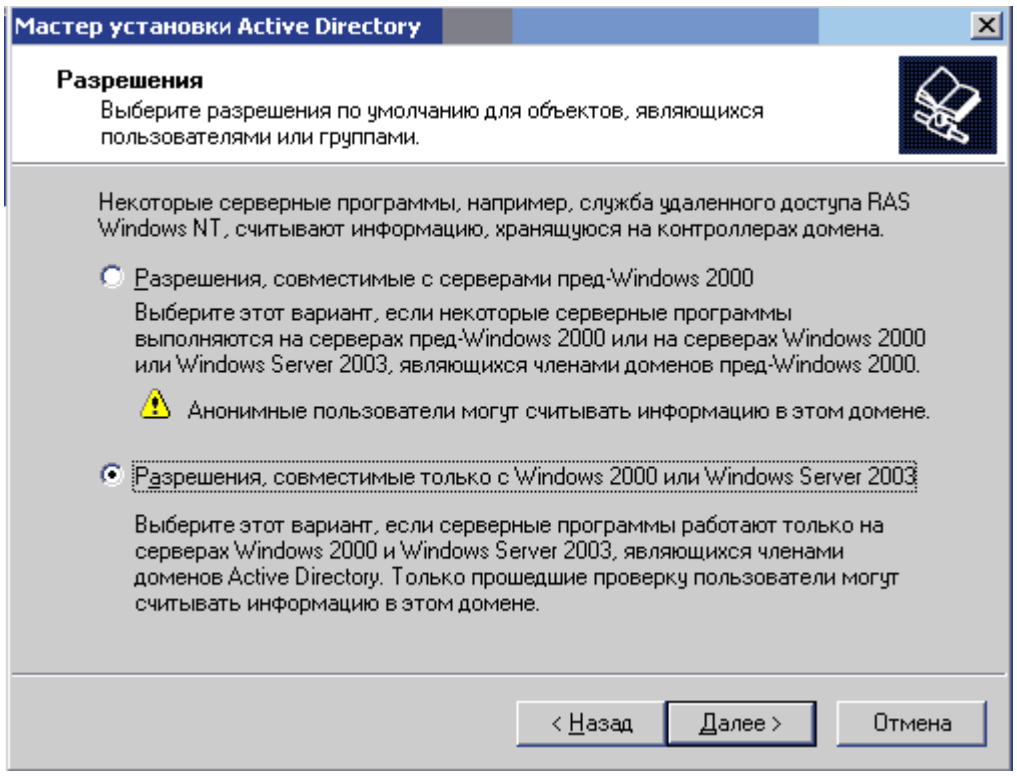


Рис. 31. Выбор требуемого уровня совместимости

После выбора одного из вариантов можно вручную переключаться между обратной совместимостью и высоким уровнем безопасности объектов Active Directory. Для этого нужно открыть компонент "Active Directory - пользователи и компьютеры" и добавить группу безопасности "Анонимный вход" в группу безопасности "Пред-Windows 2000 доступ". Для продолжения нажимаем кнопку "Далее".

На странице "Пароль администратора для режима восстановления" (рис. 32) нужно ввести и подтвердить пароль для учетной записи администратора режима восстановления для данного сервера.

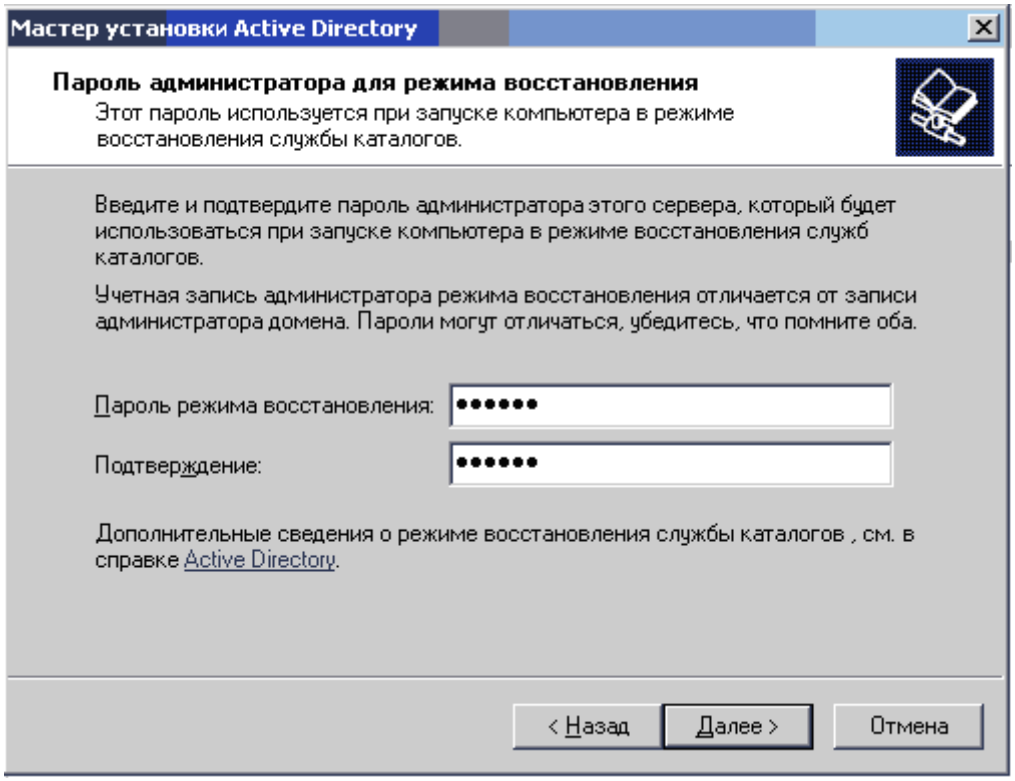


Рис. 32. Пароль администратора для режима восстановления

В качестве паролей режима восстановления каталогов необходимо использовать надежные пароли. Этот пароль необходимо знать для восстановления резервной копии состояния системы данного контроллера домена. Данный пароль нужно также использовать при запуске контроллера домена в режиме восстановления служб каталогов. Для продолжения нажимаем кнопку "Далее".

После этого просматриваем сведения на странице "Сводка", представленной на рис. 33, и нажимаем кнопку "Далее".

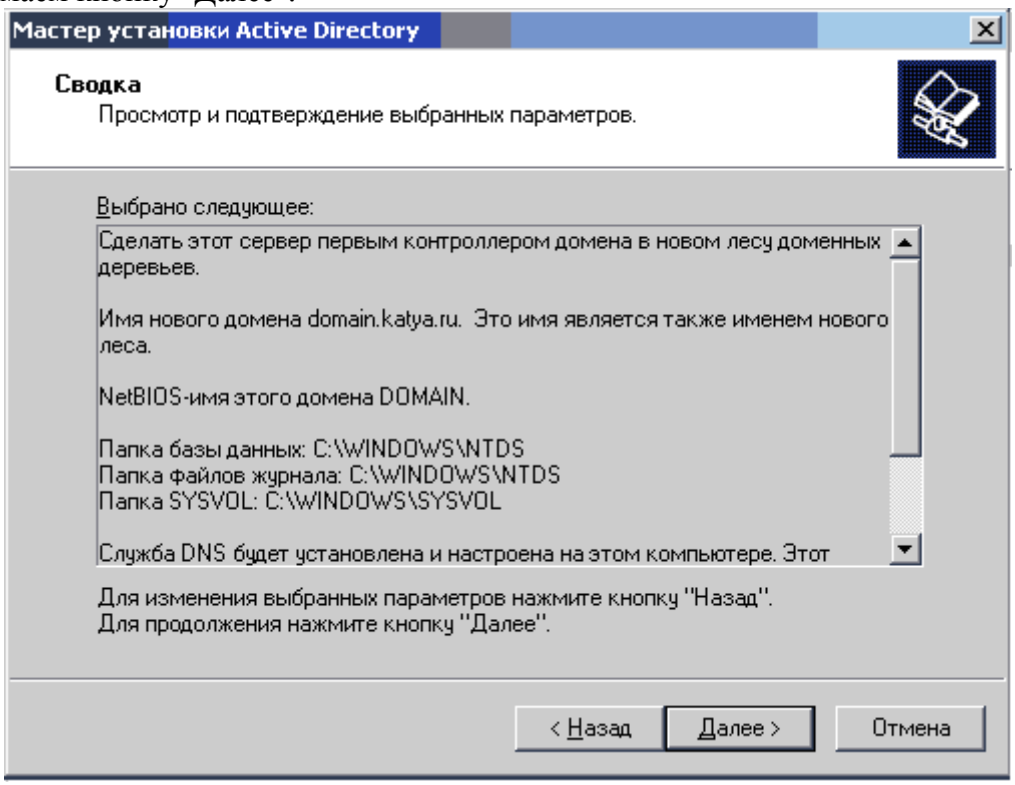



Рис. 33. Просмотр и подтверждения выбранных параметров

Мастер установки настроит Active Directory: После завершения установки нажимаем кнопку "Готово". Для перезагрузки компьютера нажимаем кнопку "Перезагрузить сейчас", чтобы изменения вступили в силу.

После перезагрузки сервера "Мастер настройки сервера" отобразит страницу "Этот сервер теперь является контроллером домена" (рис. 34).

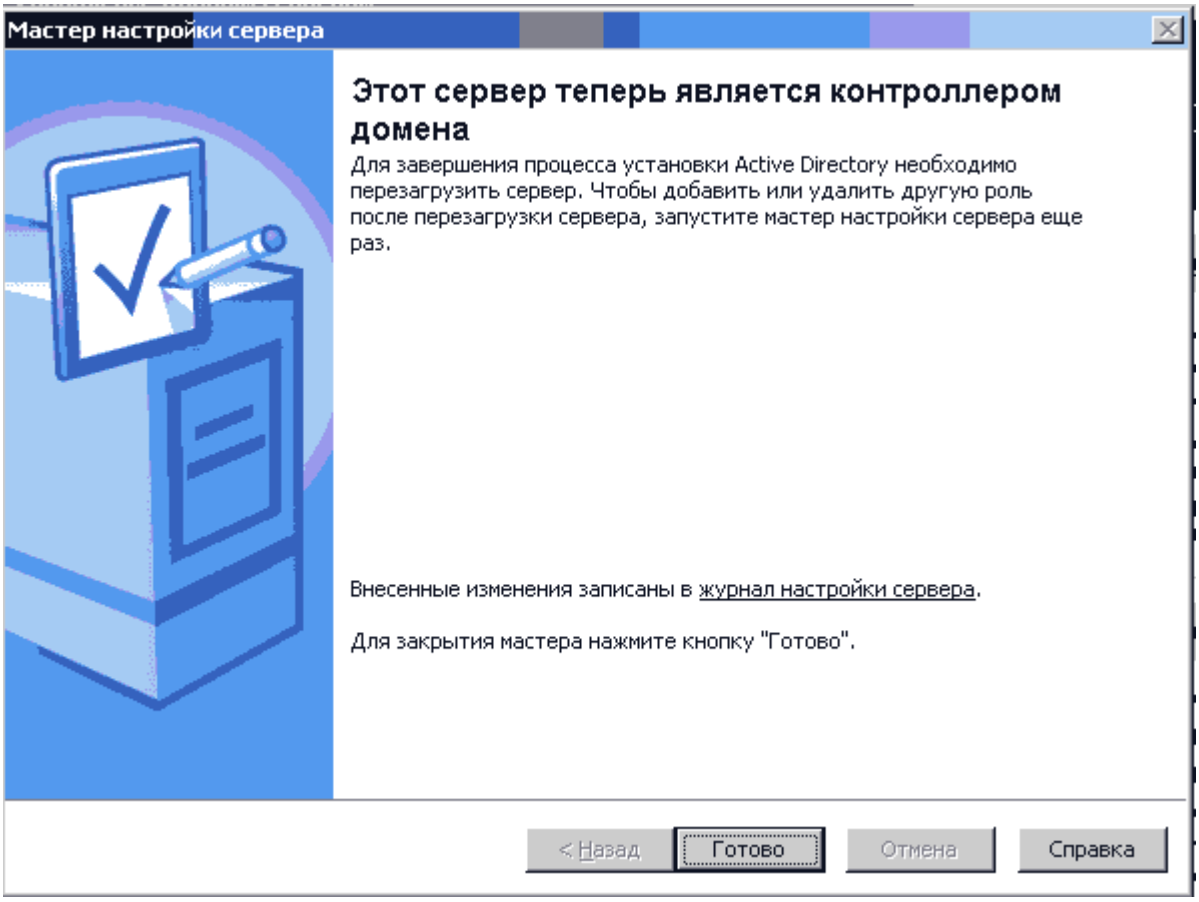



Рис. 34. Подтверждение контроллера домена

Задание: на практике осуществить установку и настройку Active Directory. Представить отчет по проделанной работе.

Контрольные вопросы:

1. Что такое каталог?
2. Что такое служба каталогов?
3. Какие элементы входят в состав службы Active Directory?
4. Охарактеризуйте понятия «дерево» и «лес». Чем они отличаются?

**Установка и настройка роли DNS**

Цель работы: приобретение студентами практических навыков установки и настройки роли DNS.

Протокол, определявший порядок обмена информацией в Интернете, описывал, в том числе и систему адресации компьютеров, объединенных в эту сеть. Согласно этой системе, каждому компьютеру присваивался уникальный четырехбайтовый адрес, который стали называть IP-адрес. Стандарт нового протокола и, соответственно, системы адресования были приняты в 1982 году. Однако человеку гораздо проще запомнить некоторое слово, чем четыре бессодержательных для него числа. Из-за этого сразу после начала работы новой сети у пользователей стали появляться списки, в которых хранились не только адреса, но и соответствующие им имена узлов. Эти данные, обычно хранившиеся в файле с именем hosts, позволяли при указании имени узла мгновенно получить его IP-адрес. Позже процесс внесения корректуры в эти файлы был усовершенствован - последнюю версию файла hosts можно было скачать с нескольких серверов с заранее определенными адресами. С ростом числа компьютеров в сети корректировать эти файлы вручную стало невозможно. Появилась необходимость в глобальной базе имен, позволяющей производить преобразование имен в IP-адреса без хранения списка соответствия на каждом компьютере. Такой базой стала DNS (Domain Name System) - система именования доменов, которая начала работу в 1987 году.

В Интернете существует множество DNS-серверов, предоставляющих клиентам необходимую информацию об именах узлов сети. Важнейшим качеством DNS является порядок их работы, поз-

воляющий DNS-серверам синхронно обновлять свои базы. Добавление адреса нового сайта в Интернете проходит за считанные часы.

Вторая особенность системы - это организация DNS-серверов в виде иерархической структуры. Например, запрос от клиента об имени ftp.microsoft.com может пройти через несколько DNS-серверов, от глобального, содержащего информацию о доменах верхнего уровня (.com, .org, .net и т. п.), до конкретного сервера компании Microsoft, в чьих списках перечислены поддомены вида *. microsoft.com, в числе которых мы и находим нужный нам ftp.microsoft.com. При этом множество DNS-серверов организуется в зоны, имеющие права и разрешения, делегированные вышестоящим сервером. Таким образом, при добавлении нового поддомена на местном сервере уведомления остальных серверов в Глобальной сети не производятся, но информация о новых серверах оказывается доступной по запросу.

Проследим прохождение запроса. При установке (точнее, при настройке) клиенту указывается как минимум один DNS-сервер (как правило, их два) - его адрес выдается провайдером. Клиент посылает запрос этому серверу. Сервер, получив запрос, либо отвечает (если ответ ему известен), либо пересылает запрос на "вышестоящий" сервер (если он известен) или на корневой (каждому DNS-серверу известны адреса корневых DNS-серверов). Так выглядит "восходящая иерархия". Затем запрос начинает спускаться вниз - корневой сервер пересылает запрос серверу первого уровня, тот - серверу второго уровня и т.д.

Помимо "вертикальных связей", у серверов есть еще и "горизонтальные" отношения - "первичный - вторичный". Действительно, если предположить, что сервер, обслуживающий какой-то домен и работающий "без страховки" вдруг перестанет быть доступным, то все машины, расположенные в этом домене, окажутся недоступны. Именно поэтому при регистрации домена второго уровня выдвигается требование указать минимум два сервера DNS, которые будут этот домен обслуживать.

Полезным свойством DNS является умение использовать "пересыльщиков" (forwarders). "Честный" DNS-сервер самостоятельно опрашивает другие сервера и находит нужный ответ, но если ваша сеть подключена к Интернету по медленной (например, dial-up) линии, то этот процесс может занимать довольно много времени. Вместо этого можно перенаправлять все запросы, скажем, на сервер провайдера, а затем принимать его ответ. Использование "пересыльщиков" может оказаться интересным и для больших компаний с несколькими сетями: в каждой сети можно поставить относительно слабый DNS-сервер, указав в качестве "пересыльщика" более мощную машину, подключенную по быстрой линии. При этом все ответы будут кэшироваться на этом мощном сервере, что ускорит разрешение имен для целой сети.

С ростом числа доменных имен работа между серверами была распределена по принципу единоначалия. Идея проста. Если организация владеет собственным доменным именем (например, microsoft.com или white-house, gov), то именование внутри своего домена она производит самостоятельно. Единственная сложность при такой работе - предоставление вышестоящими серверами этих прав нижестоящим серверам.

Уточним термины. Домен - это некий контейнер, в котором могут содержаться хосты и другие домены. Имя домена может не совпадать с именем контроллера домена, то есть домен - это виртуальная структура, не привязанная к компьютеру. Хост же, напротив, соответствует физическому компьютеру, подключенному к сети. Имя хоста является именем конкретного компьютера. Имя хоста может совпадать с именем домена. Имя домена может совпадать с именем зоны, к которой он принадлежит, в этом случае домен является корневым в зоне. При этом зона не обязана содержать в себе одноименный (корневой) домен.

Зона - это контейнер, объединяющий несколько доменов в структуру с общими разрешениями на управление, то есть зоны являются контейнерами для доменов и хостов. Зоны могут быть вложены одна в другую. Разница между зонами и доменами в том, что домену может принадлежать несколько зон, содержащих различные его поддомены. Это дает возможность делегировать полномочия для поддоменов и управлять группами поддоменов.

Зоны используются для делегирования полномочий. Каждый домен должен находиться в составе зоны при создании поддомена последний может быть переведен в новую зону, либо остав-

лен в зоне стоящего над ним домена. Для каждой зоны разрешения на создание или удаление всех входящих в нее доменов делегируются отдельно. Для нормальной работы корпоративной сети в большинстве случаев хватает единственной зоны, более того, очень часто системные администраторы ограничиваются созданием единственного домена.

Компания Microsoft рекомендует использовать DNS-серверы в корпоративных сетях для организации работы компьютеров в составе домена. Дело в том, что технология DNS более универсальна и эффективна, чем использующиеся на старых системах WINS и NetBIOS. Клиенты только посылают запросы серверу и получают ответы без обращения к каким-либо иным узлам сети.

С точки зрения производительности лучше всего интегрировать DNS в Active Directory, что возможно на серверных ОС компании Microsoft начиная с Windows 2000 Server. Совмещение ролей DNS-сервера и контроллера домена упрощает администрирование сети, особенно если размеры ее достаточно велики.

Итак, DNS-серверы поддерживают записи в распределенной базе данных DNS и используют эти записи для обработки запросов сопоставления DNS-имен, созданных DNS-клиентами, таких как запросы имен веб-сайтов или компьютеров в сети или в Интернете. Если планируется использовать компьютер для обработки DNS-запросов компьютеров в сети, следует добавить для него роль DNS-сервера.

Операционная система Windows Server 2003 позволяет настроить сервер как DNS-сервер. Для этого нам необходимо выполнить следующие действия: открыть оснастку "Управление данным сервером"; выбрать ссылку Добавить или удалить роль; на странице Предварительные шаги прочитать информацию о сетевых соединениях и подтвердить, что все они доступны; на странице Параметры настройки выбрать вариант Особая конфигурация.

На экран будет выведена новая страница - Роль сервера (рис. 57).

На этой странице мы выбираем из списка DNS-сервер и нажимаем кнопку "Далее". Появится страница "Сводка выбранных параметров", представленная на рисунке 58, на которой можно просмотреть и подтвердить выбранные параметры.

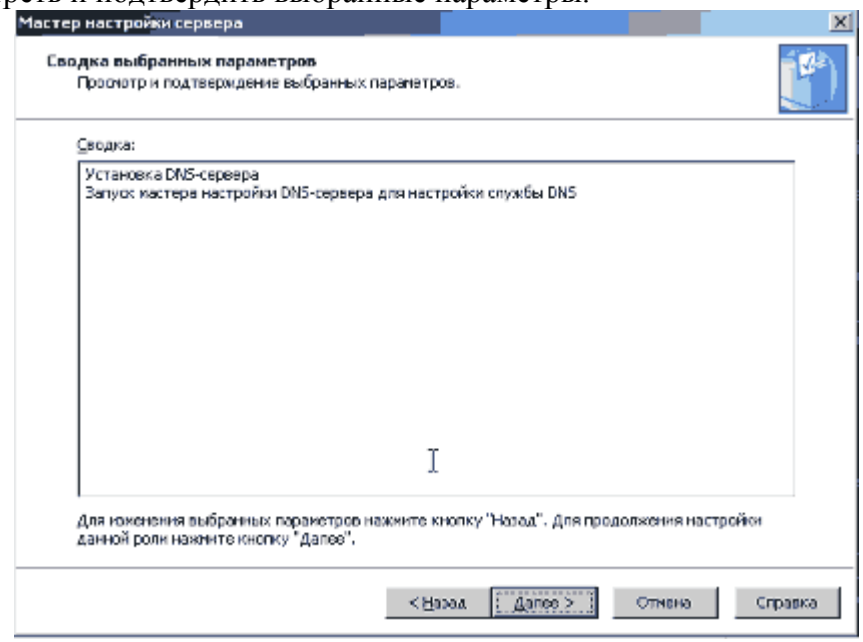



Рис. 58. Сводка выбранных параметров

Для применения параметров, выбранных на странице "Сводка выбранных параметров", нажимаем кнопку "Далее". Появится страница "Применение выбранных параметров" (рис. 59), которая будет находиться на экране всё время до окончания установки и настройки DNS-сервера.

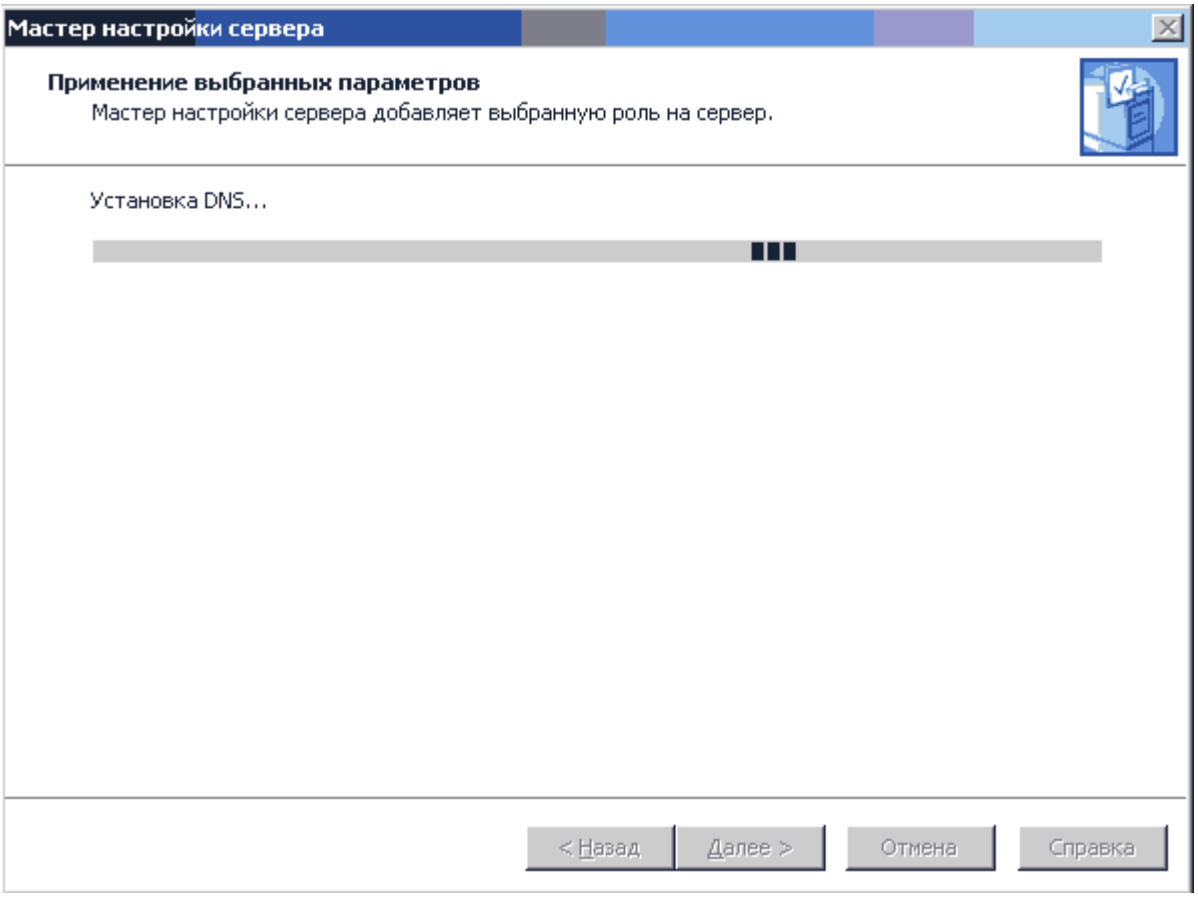



Рис. 59. Применение выбранных параметров

Мастер настройки сервера установит службу DNS-сервер. В процессе установки службы DNS-сервера мастер настройки сервера определяет, является ли IP-адрес для этого сервера статическим или настраивается автоматически. Клиенты DNS находят DNS-серверы при помощи автоматически настраиваемых статических IP-адресов. Это может создавать трудности для клиентов DNS при изменении IP-адресов.

Если этот сервер настроен для автоматического получения IP-адреса, то появляется окно "Настройка компонентов" мастера компонентов Windows и предлагает настроить этот сервер для использования статического IP-адреса.

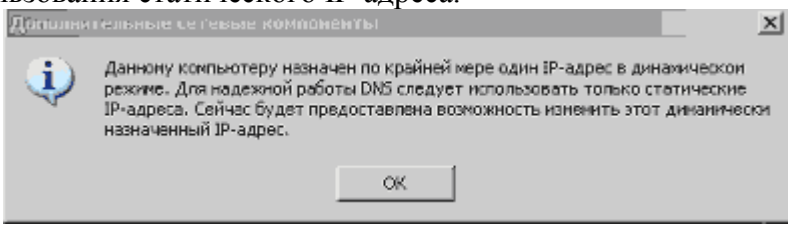



Рис. 60. Дополнительные сетевые компоненты

На странице "Подключение по локальной сети - свойства" (рис. 61) мы выбираем вариант "Протокол Интернета (TCP/IP)" и нажимаем кнопку "Свойства" (или дважды щелкаем по нему левой кнопкой мыши).

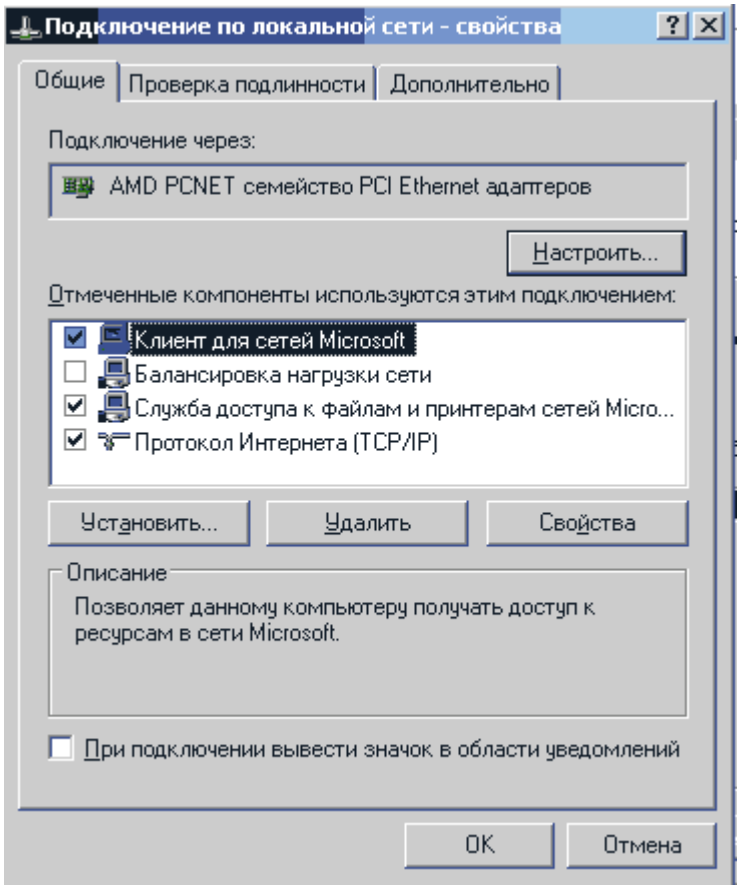


Рис. 61. Подключение по локальной сети - свойства

В диалоговом окне "Свойства: Протокол Интернета (TCP/IP)" (рис. 62) выбираем "Использовать следующий IP-адрес" и вводим статический IP-адрес, маску подсети и основной шлюз для этого сервера:

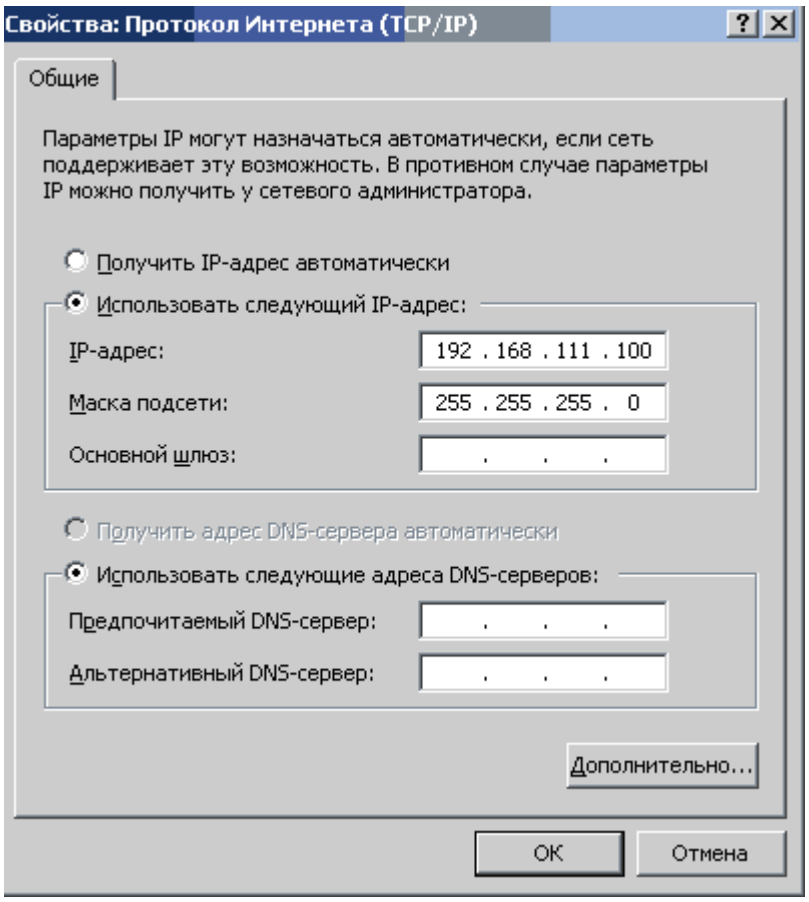


Рис. 62. Свойства: Протокол Интернета (TCP/IP)

В строке "Предпочитаемый DNS-сервер" вводим IP-адрес этого сервера, а в строке "Дополнительный DNS-сервер" - IP-адрес DNS-сервера, находящегося в центральном офисе или у поставщика услуг Интернета. После настройки статических IP-адресов для DNS-сервера нужно нажать кнопку OK, а затем - кнопку "Закрыть".

Для небольшой организации статический IP-адрес сервера будет использоваться для регистрации DNS-имени домена авторизованным регистратором Интернета. Регистратор Интернета сопоставит DNS-имя домена организации с IP-адресом, и компьютерам в Интернете при поиске компьютеров из сети организации будет известен IP-адрес DNS-сервера этой сети.

Для подразделения статический IP-адрес сервера будет использоваться при делегировании имени домена, настроенного на DNS-сервере в центральном офисе организации. Компьютеры в организации и в Интернете при поиске компьютеров из сети будут использовать IP-адрес DNS-сервера этой сети. Поэтому очень важно не изменять IP-адрес этого сервера после добавления роли DNS-сервера.

После нажатия кнопки "Закрыть" запускается "Мастер настройки DNS-сервера", представленный на рисунке 63.

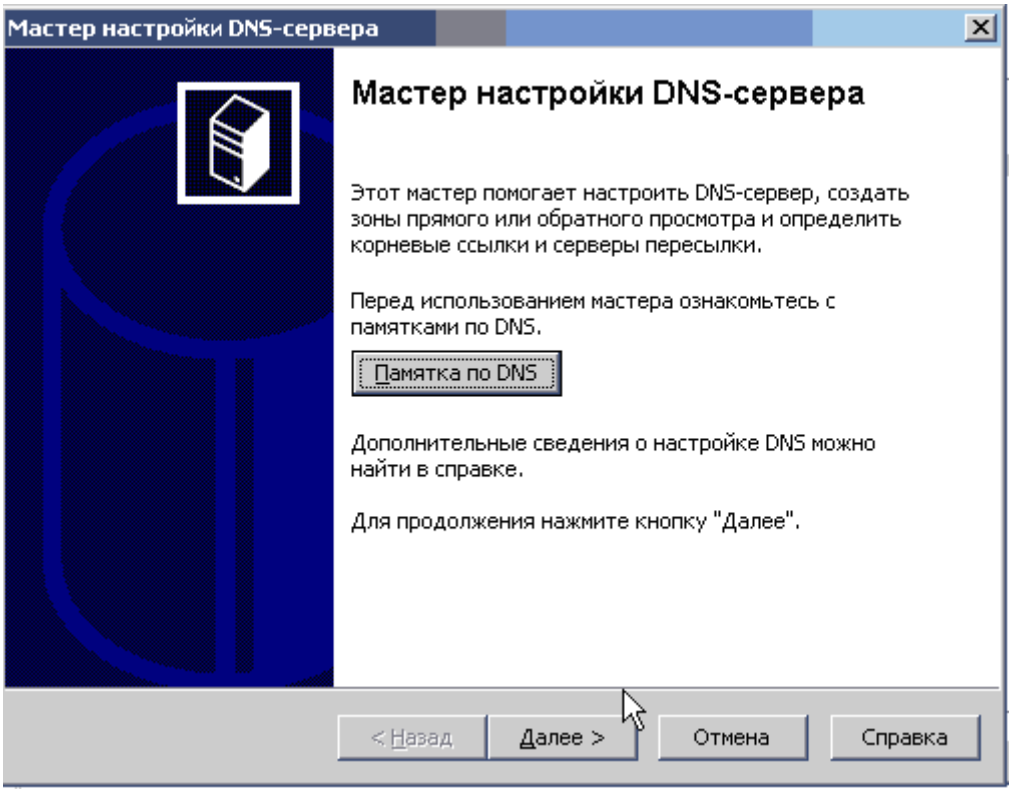



Рис. 63. Мастер настройки DNS-сервера

Если отменить работу мастера настройки DNS-сервера, служба DNS-сервера останется установленной, но не сможет рассылать клиентам IP-адреса, пока не будет создана область. Создать область позже можно при помощи консоли DNS. Для продолжения нужно нажать "Далее".

На странице "Выбор действия по настройке" (рис. 64) выбираем вариант "Создать зону прямого просмотра" и нажимаем кнопку "Далее".

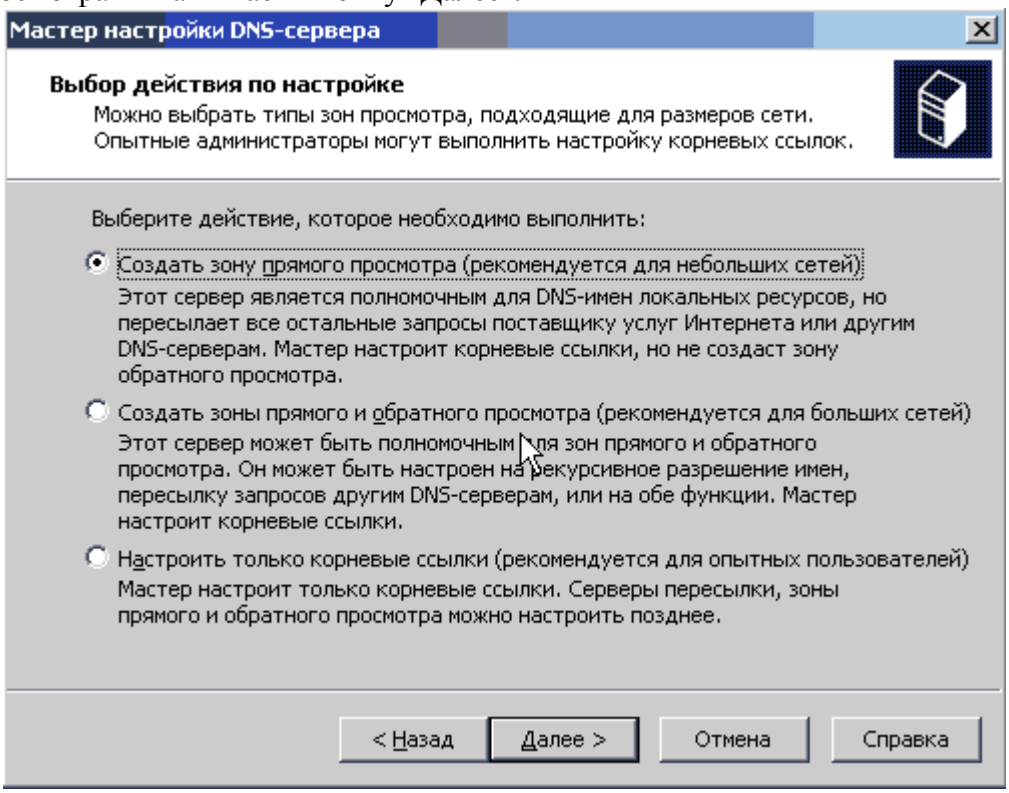



Рис. 64. Выбор действия по настройке

Чтобы задать, что этот DNS-сервер будет содержать зону DNS, в которую входят записи ресурсов DNS для ресурсов сети, на странице "Размещение основного сервера" мы выбираем "Управление зоной выполняется этим сервером" и нажимаем кнопку "Далее" (рис. 65).

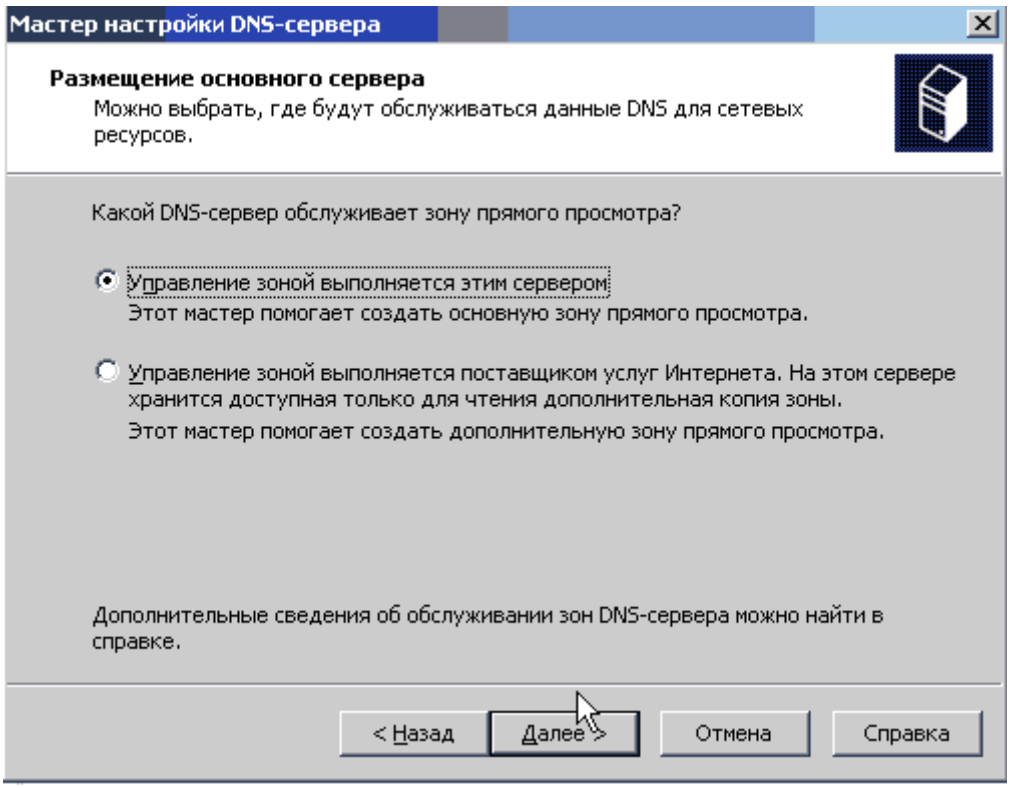



Рис. 65. Размещение основного сервера

На странице "Имя зоны" (рис. 66) в строке "Имя зоны" задаём имя зоны DNS для сети и нажимаем кнопку "Далее".

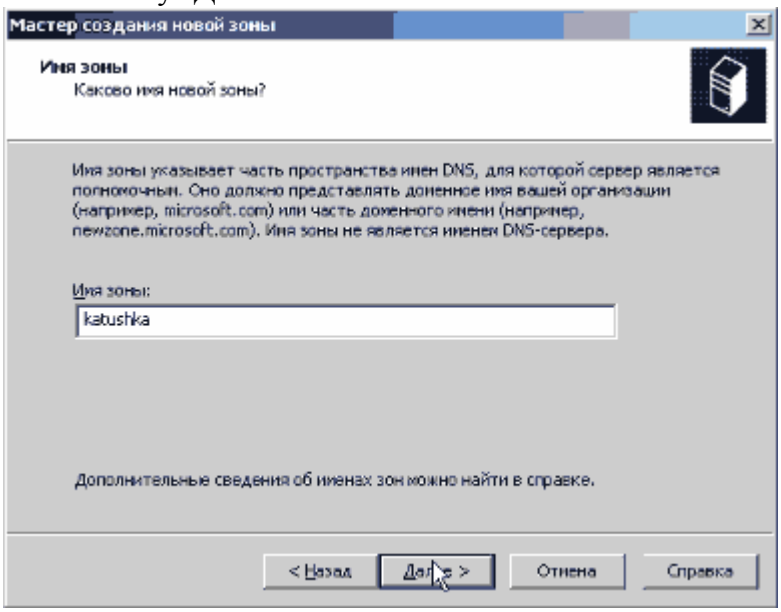



Рис. 66. Задаем имя зоны

Имя зоны совпадает с именем DNS-домена для небольшой организации или подразделения.

На странице "Файл зоны" (рис. 67) будет предложено создать новый файл зоны или скопировать существующий с другого DNS-сервера.

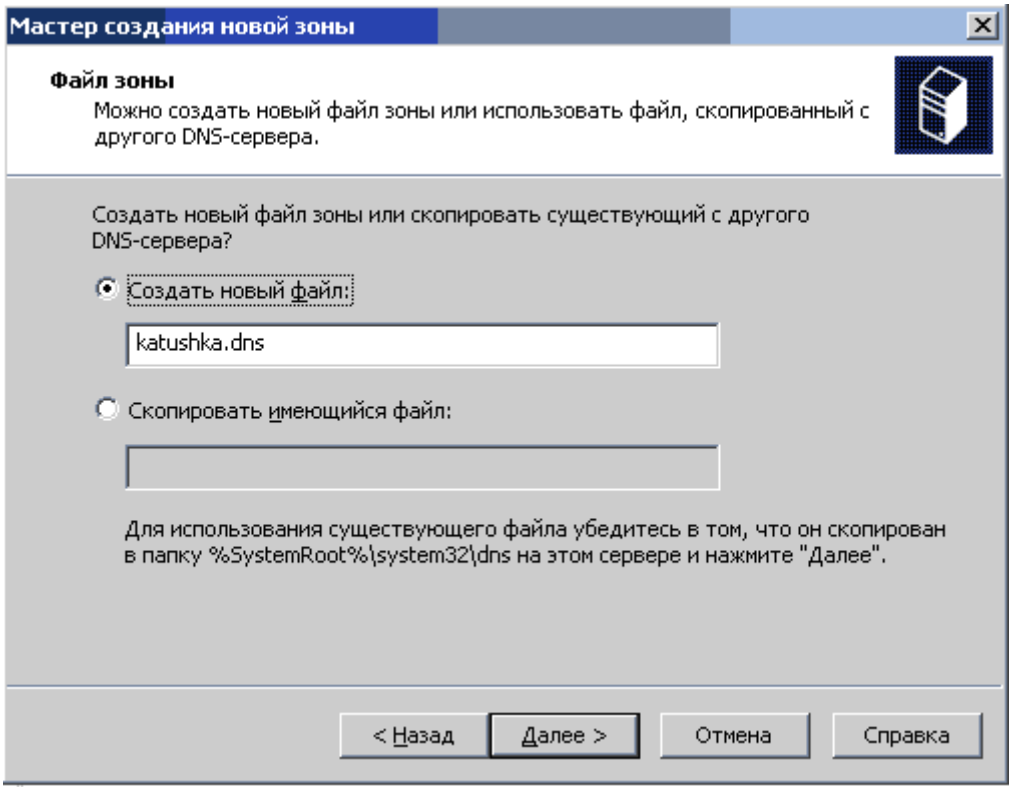



Рис. 67. Файл зоны

Выбираем "Создать новый файл" и нажимаем "Далее".

На странице "Динамическое обновление" (рис. 68) можно определить, будет ли данный DNS-сервер принимать динамические обновления. Если выбрать вариант "Разрешить любые динамические обновления", можно автоматизировать процесс обновления записей ресурсов DNS для ресурсов сети, но этот вариант опасен, так как обновления могут быть получены от источников, не заслуживающих доверия. Мы выбираем "Запретить динамическое обновление" и нажимаем "Далее".

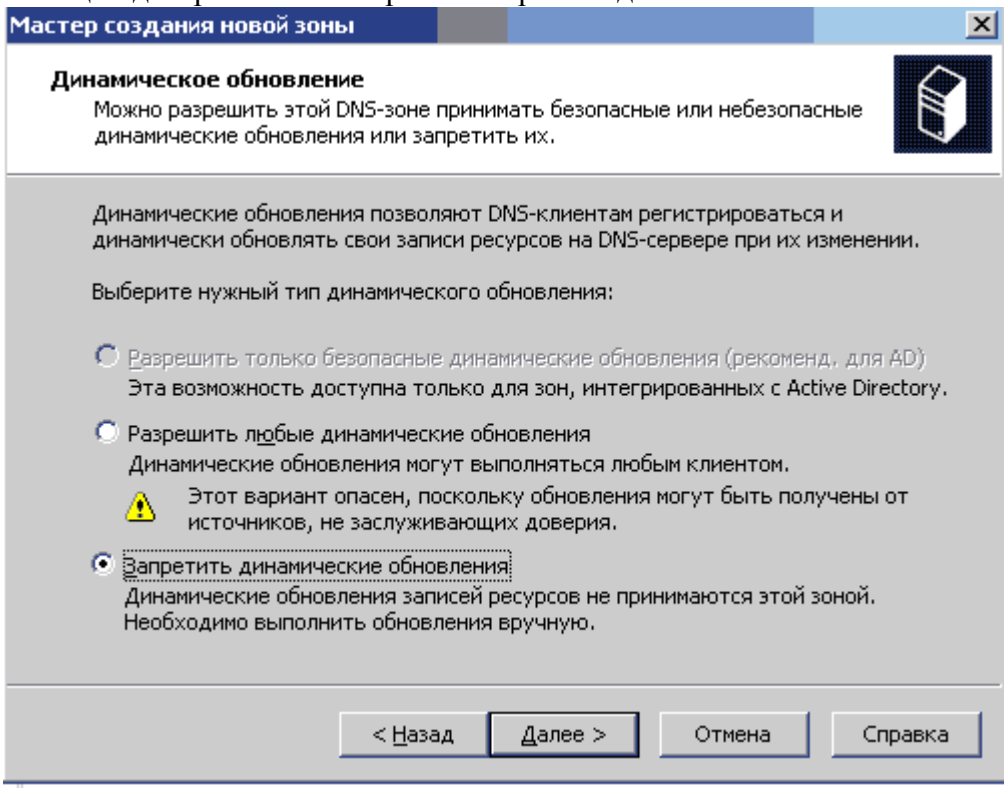



Рис. 68. Динамическое обновление

На странице "Серверы пересылки", представленной на рисунке 69, будет предложено указать IP-адреса DNS-серверов, которым данный DNS-сервер будет пересылать запросы, на которые он сам не в состоянии ответить.

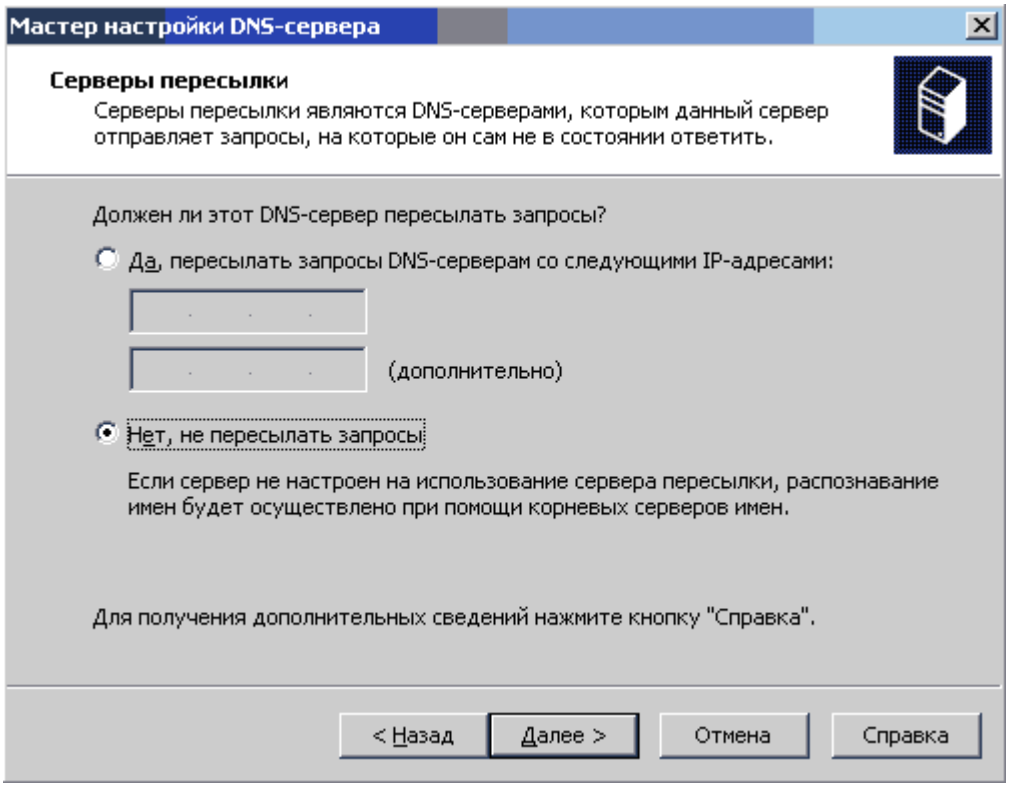



Рис. 69. Серверы пересылки

Выбор конфигурации позволит пересылать запросы DNS для DNS-имен вне сети на DNS-сервер центрального офиса или поставщика услуг Интернета. Введите один или несколько IP-адресов, используемых DNS-серверами центрального офиса или поставщика услуг Интернета. Мы выбираем "Нет, не пересылать запросы" и нажимаем "Далее". Мастер настройки DNS-сервера осуществит поиск корневых ссылок и выведет на экран страницу "Завершение работы мастера настройки DNS-сервера" (рис. 70).

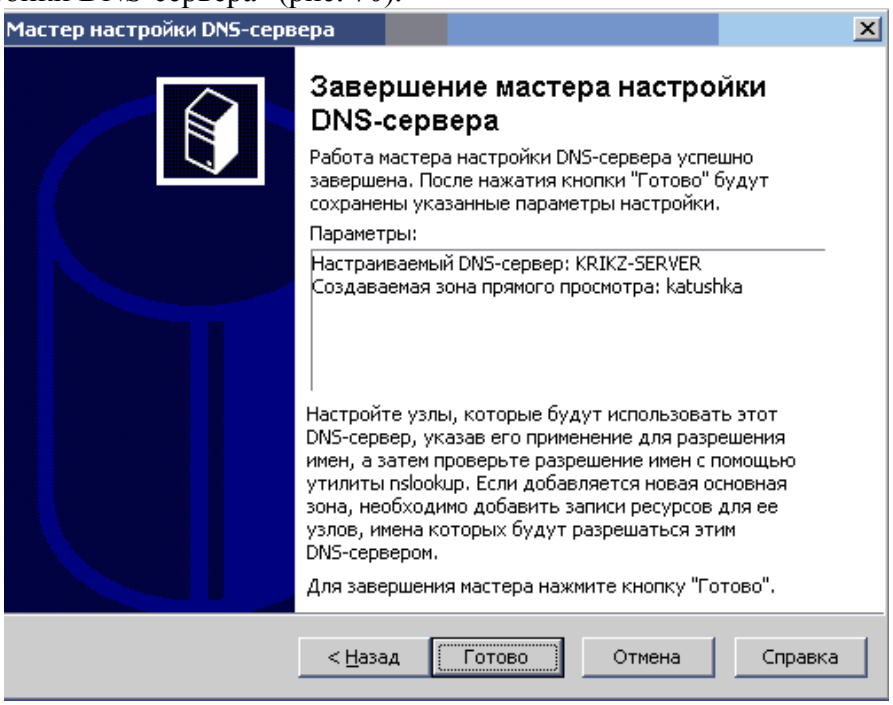



Рис. 70. Завершение работы мастера настройки DNS-сервера

На этой странице можно нажать кнопку "Назад" для изменения любого параметра. Для применения выбранных нами параметров нажимаем кнопку "Готово". После завершения работы мастера настройки DNS-сервера на экране будет отображена страница "Этот сервер теперь является DNS-сервером" (рис. 71).

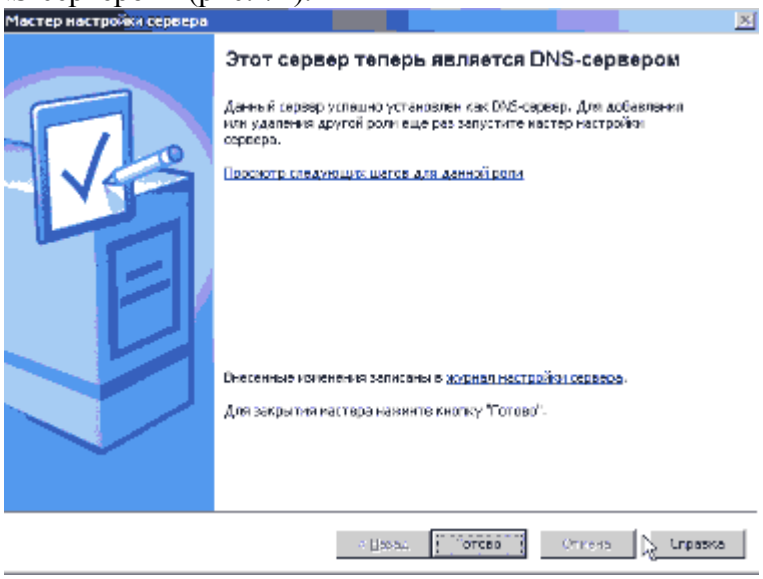



Рис. 71. Этот сервер теперь является DNS-сервером

После завершения работы мастера настройки сервера и мастера настройки DNS-сервера DNS-сервер готов к использованию.

При завершении работы мастера настройки сервера автоматически устанавливается консоль DNS, которая используется для управления DNS-сервером. Чтобы открыть компонент "DNS" (рис. 72), нужно нажать кнопку "Пуск", выбрать команду "Программы - Администрирование", а затем - "DNS".

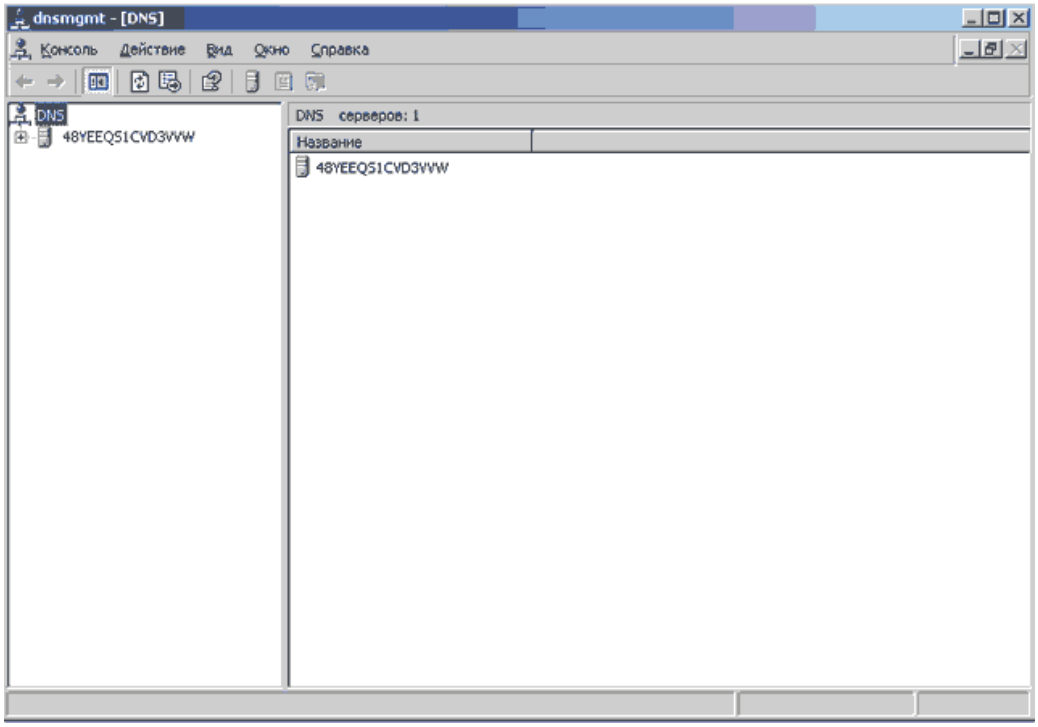



Рис. 72. Компонент DNS

Задание:

На практике осуществить установку DNS –сервера. Представить отчет о проделанной работе

Контрольные вопросы:

1. Что такое DNS

2. Опишите основные особенности системы
3. Что такое зона, домен? Чем отличаются эти понятия?

## 4. Методические указания к самостоятельной работе студентов

Самостоятельная работа по дисциплине «Администрирование информационных систем», направлена на углубление и закрепление знаний студента, на развитие практических умений и включает в себя следующие виды работ:

– работа с лекционным материалом, учебниками и учебными пособиями;
– изучение тем, вынесенных на самостоятельную проработку;
– подготовка к практическим занятиям;
– выполнение домашних индивидуальных заданий;
– подготовка к лабораторным работам;
– подготовка к текущему и итоговому контролю.