Министерство общего и профессионального образования

Калининградский Государственный Университет

Центр дополнительного профессионального образования

*Аттестационная работа по теме:*

***"Администрирование корпоративной сети на основе  
 Microsoft Windows 2000 Advanced Server "***

Выполнила \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Корнышева И.В./

Проверил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Молчанов С.В./

Калининград 2003 г.

**Содержание**

[ВВЕДЕНИЕ 5](#_Toc45946676)

[1. проектирования корпоративной сети 6](#_Toc45946677)

[1.1. Особенности проектирования корпоративных сетей 6](#_Toc45946678)

[1.2. Этапы проектирования корпоративных сетей 7](#_Toc45946679)

[1.2.1. Анализ требований 8](#_Toc45946680)

[1.2.2. Построение функциональной модели производства 9](#_Toc45946681)

[1.2.3. Построение технической модели 9](#_Toc45946682)

[2.1. Информационные потоки в ЛВС предприятия 11](#_Toc45946683)

[3. Выбор операционной системы. 12](#_Toc45946684)

[3.1 Обзор операционных систем 12](#_Toc45946685)

[3.1.1 ОС Nowell NetWare 12](#_Toc45946686)

[3.1.2. Семейство ОС Windows 2000. 15](#_Toc45946687)

[3.1.2.1 Windows 2000 Server 15](#_Toc45946688)

[3.1.2.2 Windows 2000 Advanced Server 16](#_Toc45946689)

[3.1.2.3 Windows 2000 Datacenter Server 16](#_Toc45946690)

[3.1.3. ОС Windows Server 2003. 16](#_Toc45946691)

[3.1.4. ОС Unix, Linux 17](#_Toc45946692)

[3.2. Обоснование выбора Операционной системы Windows 2000 Advanced Server . 19](#_Toc45946693)

[4. Планирование структуры сети 24](#_Toc45946694)

[4.1. Способ управления сетью 24](#_Toc45946695)

[4.2. Размещение сервера 26](#_Toc45946696)

[4.3. Сетевая архитектура 27](#_Toc45946697)

[4.4. Сетевые ресурсы 30](#_Toc45946698)

[5. Организация сети на основе Windows 2000. 33](#_Toc45946699)

[5.1. Служба каталогов Windows 2000 33](#_Toc45946700)

[5.1.1. Наименование объектов 33](#_Toc45946701)

[5.1.2. Логическая структура Active Directory 35](#_Toc45946702)

[5.1.2.1. Домены 35](#_Toc45946703)

[5.1.2.2 Дерево 36](#_Toc45946704)

[5.1.2.3 Лес 37](#_Toc45946705)

[5.1.2.4 Организационные единицы 38](#_Toc45946706)

[5.1.3. Физическая структура 39](#_Toc45946707)

[5.1.3.1 Сайты 39](#_Toc45946708)

[5.1.3.2 Контроллеры доменов 40](#_Toc45946709)

[5.2. Служба DHCP. 44](#_Toc45946710)

[5.2.1. Настройка службы DHCP. 47](#_Toc45946711)

[5.2.2. Кластеризация 52](#_Toc45946712)

[5.3. Служба DNS 53](#_Toc45946713)

[5.3.1. Планирование внедрения DNS для Active Directory 57](#_Toc45946714)

[5.3.2. Новые свойства DNS в Windows 2000 60](#_Toc45946715)

[5.3.3 Настройка сервера DNS. 62](#_Toc45946716)

[5.4. Служба WINS 63](#_Toc45946717)

[5.4.1. Новые возможности WINS в Windows 2000 64](#_Toc45946718)

[5.4.2. Компоненты службы WINS 65](#_Toc45946719)

[5.4.3. Планирование сети с использованием WINS 66](#_Toc45946720)

[5.4.4. Управление базой данных WINS 67](#_Toc45946721)

[5.5. Конфигурирование сервера 69](#_Toc45946722)

[5.5.1. Выбор сервера 69](#_Toc45946723)

[5.5.2. Установка Windows 2000 Advanced Server 73](#_Toc45946724)

[5.5.2.1. Запуск процедуры предварительного копирования файлов и текстового режима Windows 2000 Advanced Server 73](#_Toc45946725)

[5.5.2.2. Графический режим установки и сбор информации 75](#_Toc45946726)

[5.5.2.3. Завершение установки оборудования 77](#_Toc45946727)

[5.5.3. Управление в среде Windows 2000 Advanced Server 78](#_Toc45946728)

[5.5.4. Требования к домену 79](#_Toc45946729)

[5.5.5. Выбор модели организации сети 80](#_Toc45946730)

[5.6. Служба Routing and Remote Access 81](#_Toc45946731)

[5.7. Измерение сетевого трафика 82](#_Toc45946732)

[6. Защита информации в сети 84](#_Toc45946733)

[6.1. Анализ возможностей системы разграничения доступа Windows 2000 Advanced Server 85](#_Toc45946734)

[6.1.1. Слежение за деятельностью сети 85](#_Toc45946735)

[6.1.2. Начало сеанса на рабочей станции 86](#_Toc45946736)

[6.1.3. Учетные карточки пользователей 86](#_Toc45946737)

[Logon hours 87](#_Toc45946738)

[6.1.4. Журнал событий безопасности 88](#_Toc45946739)

[6.1.5. Права пользователя 91](#_Toc45946740)

[6.1.6. Установка пароля и политика учетных карточек 92](#_Toc45946741)

[6.1.7. Шифрованная файловая система EFS 93](#_Toc45946742)

[Заключение 95](#_Toc45946743)

[Список использованной литературы 98](#_Toc45946744)

ВВЕДЕНИЕ

В данной аттестационной работе рассматривается проблема построения локальной вычислительной сети организации под управлением операционной системы Windows 2000 Advanced Server.

Реализация предложенного проекта позволит сократить бумажный документооборот внутри подразделения, повысить производительность труда, сократить время на обработку информации. Как следствие, образуются дополнительные временные ресурсы для разработки и реализации новых экономических и инвестиционных проектов. Таким образом, решится проблема окупаемости и рентабельности внедрения корпоративной сети.

Локальная вычислительная сеть должна быть спроектирована таким образом, чтобы обеспечить надлежащую степень защищенности данных.

Целью аттестационной работы является организация корпоративной компьютерной сети.

Для решения поставленной цели в работе решаются следующие задачи:

* выбор операционной системы;
* выбор способа управления сетью;
* управление сетевыми ресурсами и пользователями сети;
* рассмотрение вопросов безопасности сети;

Необходимо разработать рациональную, гибкую структурную схему сети предприятия, выбрать аппаратную и программную конфигурацию сервера, а так же проработать вопросы обеспечения необходимого уровня защиты данных.

# 1. проектирования корпоративной сети

Корпоративная сеть обслуживает одно крупное предприятие и называется также сетью масштаба предприятия. Структура корпоративной сети выглядит следующим образом: имеется ряд подсетей, представляющих собой ЛВС типа Ethernet или Token Ring и обслуживающих каждая отдельное подразделение, расположенное в одной или нескольких близкорасположенных комнатах; подсети связаны между собой с помощью *серверов доступа*; обычно имеется выход во внешнюю территориальную сеть. В качестве серверов доступа могут использоваться мосты, коммутаторы, маршрутизаторы, шлюзы. [5]

## 1.1. Особенности проектирования корпоративных сетей

При проектировании корпоративной сети полезно ее представление в виде многослойной пирамиды. Хотя слои этой пирамиды связаны и оказывают непосредственное влияние друг на друга, обычно каждый слой проектируется достаточно автономно, специалистами и фирмами соответствующего профиля.

В зависимости от направления движения по этой пирамиде: сверху вниз - от бизнес-приложений к аппаратной платформе, или снизу вверх - от аппаратуры к приложениям, или от середины - от конкретной СУБД, - все фирмы, работающие в области сетевой интеграции, можно условно разделить на три группы:

Фирмы-производители или дистрибьюторы аппаратуры, выступающие в роли интеграторов. У этих интеграторов пирамида опирается на очень узкое основание из одной платформы от одного-двух производителей. Минусы и некоторые плюсы в работе такого интегратора достаточно очевидны.

Фирмы, ориентирующиеся на одну из СУБД, например, только на Oracle или Informix. В этом случае узким местом пирамиды является середина: при попытке использовать несколько аппаратных платформ и широкий спектр прикладного программного обеспечения, ограничения диктуются используемой СУБД.

Наконец, третья группа - независимые интеграторы, которые могут предлагать любые решения на каждом из уровней пирамиды и которых нельзя уличить в особой привязанности к определенной платформе, сетевым конфигурациям или приложениям. У таких интеграторов единственным критерием выбора каждого конкретного решения в идеале является требование достижения максимального эффекта в рамках заданных ресурсов. В таком случае есть возможность гибко строить любые конфигурации, что позволяет достаточно просто решать проблемы, связанные с тем, что заказчик уже использует, например, какую-либо СУБД и не хочет переучивать свой персонал для работы с другой базой данных.

При этом, при проектировании какого-либо слоя характеристики других слоев, оказывающих влияние на принятие проектных решений, берутся в виде исходных данных, чаще всего в весьма обобщенном виде. Например, при проектировании приложений учитываются скорости, которые может обеспечить сегодняшнее коммуникационное оборудование вполне определенного диапазона стоимости - того диапазона, который имеется в распоряжении предприятия. И наоборот, разработчики транспортной системы ориентируются на усредненные данные о трафике, который могут создать имеющиеся на предприятии приложения и те приложения, которые намечено ввести в действие в ближайшие год-два. [9]

## 1.2. Этапы проектирования корпоративных сетей

При проектировании любой ЛВС существуют типовые этапы выполнения сетевых проектов.

### 1.2.1. Анализ требований

Анализ требований к сети поможет оценить деловую значимость информационно-технологических решений, определить главные цели и выбрать приоритеты для отдельных частей компьютерной системы, которую вы хотите улучшить или расширить. Четкое определение требований к функциям сети поможет избежать реализации не нужных свойств сети, что сэкономит средства вашего предприятия. Тщательный анализ требований к сети является основой для написания хорошего технического задания, на базе которого системные интеграторы смогут разработать проект сети. Наконец, ясное понимание целей поможет сформулировать критерии качества для оценки и тестирования реализованной сети.

На этом этапе формулируются основные деловые цели предприятия, для которого разрабатывается проект, например, сокращение производственного цикла, более оперативный прием заказов или повышение производительности труда за счет более эффективного взаимодействия сотрудников, то есть те цели предприятия, которые в настоящий момент, при существующих средствах и технологиях не вполне достигаются. Осуществляется поиск аналогичных систем, анализируются их сильные и слабые стороны, определяется возможность использования удачного опыта для проектируемой системы.

Для выполнения анализа требований к корпоративной сети необходимо:

оценить текущее состояние локальных сетей и парка компьютеров на предприятии, что поможет выявить, какие проблемы требуют решения;

* определить цели и выгоды от корпоративной сети, что поможет вам правильно спроектировать сеть;
* обосновать перед руководством предприятия необходимость покупок;
* написать эффективное техническое задание;
* определить критерии для оценки качества сети. [9]

### 1.2.2. Построение функциональной модели производства

Сеть предприятия предназначена для того, чтобы выполнять производственные функции, поэтому следует оценить ее роль в производственной структуре предприятия. Для успешного построения корпоративной сети нужно построить функциональную модель (или, по-другому, бизнес-модель), из которой потом получить техническую и физическую модели сети.

Бизнес-модель описывает деловые процедуры, последовательность и взаимозависимость всех выполняемых на предприятии работ. При этом внимание концентрируется не на компьютерной системе, а концентрируется на деловой практике и последовательности работ.

Архитектура приложений и вычислительной системы играет ключевую роль в деловой архитектуре предприятия. Бизнес предприятия базируется на архитектуре управления данными, на приложениях и архитектуре сети. Успешный анализ требований и успешное построение корпоративной сети требуют от технического специалиста умения думать как бизнесмен.

### 1.2.3. Построение технической модели

После разработки бизнес-модели предприятия и определения того, какие процедуры требуют изменения или улучшения, необходимо построить техническую модель сети. Техническая модель описывает в достаточно общих терминах, какое компьютерное оборудование нужно использовать, чтобы достичь целей, определенных в бизнес-модели. Чтобы построить техническую модель, нужно проанализировать существующее оборудование, определить системные требования, оценить сегодняшнее и завтрашнее состояния техники.

Проектировщик также должен обеспечить нужный набор функций и требуемое время доступности сети. Например, если сеть должна быть доступна по ночам и в выходные дни, в ответственных файл-серверах нужно предусмотреть избыточные диски и источники бесперебойного питания. Необходимо решить, достаточно ли применение способа зеркального отображения дисков или требуется использовать дисковый массив. [10]

Далее нужно выяснить, какие технологии и технические средства станут доступными в ближайшее время, а также каковы долгосрочные перспективы этих новшеств. Необходимо оценить, сможет ли проектируемая сеть принять завтрашние технологические новинки.

Искусство проектировщика заключается в оценке имеющихся на сегодня решений, предвидении того, что станет доступным завтра, и объединении этих решений в элегантную и эффективную сеть.

После того, как выбрана техническая модель, описывающая сеть в общих терминах, создается так называемая физическая модель, которая является подробным описанием конкретных продуктов, их количества, технических параметров и способов взаимодействия.

Установка и наладка системы. Данный этап подразумевает координирование поставок от субподрядчиков, управление конфигурированием, инсталляцию и наладку оборудования, обучение персонала.

Тестирование системы. На этом этапе должны проводиться приемочные испытания.

Сопровождение и эксплуатация системы. Этот этап не имеет четко определенных временных границ, а представляет собой непрерывный процесс. [5]

# 2.1. Информационные потоки в ЛВС предприятия

Рассмотрим организационно-штатную структуру подразделения. Во главе подразделения стоит генеральный директор предприятия. В состав подразделения входят 4 отдела, один из которых - специализированный отдел прямого подчинения начальнику. Каждый отдел имеет в подчинении разное количество отделений. В каждом отделении, в свою очередь, служат сотрудники согласно штатно-списочного расписания.

Все вышесказанное иллюстрирует рис. 2.1.

|  |
| --- |
| 1-й  отдел  Директор  Отдел прямого подчинения  2-й отдел  3-й отдел  4-й отдел  6-е отделение  5-е отделение  4-е отделение  2-е отделение  1-е отделение  3-е отделение  - распоряжения  - оперативная информация  - доклады |

Рис. 1.1. Организационная структура подразделения

Всего в подразделении задействовано 30 человек, каждому из которых предполагается выделить в пользование персональный компьютер.

# 3. Выбор операционной системы.

## 3.1 Обзор операционных систем

Практически все современные ОС поддерживают работу в сети. Однако в качестве ОС для сервера чаще всего используются Nowell NetWare, Unix, Linux и Windows 2000 Server.

### 3.1.1 ОС Nowell NetWare

Одна из первых коммерческих сетевых ОС, позволивших строить сети произвольной топологии, состоящих из разнородных компьютеров. Если раньше сетевые ОС сильно зависели от конкретной конфигурации сети, то ОС Nowell NetWare стала первой универсальной сетевой ОС. Любая сетевая карта, имеющая драйвер ODI (Open Datalink Interface) может использоваться в сетях Nowell. Благодаря такой универсальности ОС быстро завоевала рынок, и долгое время оставалась основной ОС для локальных сетей. С 1990 года даже фирма IBM стала перепродавать NetWare, и по сегодняшний день эта ОС используется достаточно широко.

Текущей версией ОС является NetWare 6.x. Помимо удобного графического интерфейса, эта версия NetWare имеет ряд других характерных особенностей:

1) NetWare 6.0 использует в качестве основного сетевого протокола TCP/IP (протокол, используемый в сети Internet). Если предыдущие версии NetWare работали на собственном протоколе фирмы Novell - протоколе IPX/SPX, а протокол ТСР/IР мог использоваться только поверх IPX/SPX (также эмулировался NetBIOS), то теперь NetWare 5.0 предлагает следующие варианты:

- только протокол TCP/IP

- протокол TCP/IP в режиме "совместимости" (может использоваться IPX/SPX поверх ТСР/IР)

- совместное использование протоколов TCP/IP и IPX/SPX (оба протокола работают параллельно и

независимо)

- только протокол IPX/SPX.

2) В NetWare используется служба каталога NDS (Nowell Directory Service), которая представляет собой единую распределенную базу данных в виде дерева каталогов, в которой описываются все объекты сети (пользователи, группы пользователей, принтеры и т.д.), с указаниями прав доступа. База данных NDS является общей для всей сети. Если в предыдущих версиях NetWare 3.x и 2.x необходимо было создавать учетную запись пользователя (имя и пароль) на каждом сервере сети, то в NetWare 6.0 достаточно один раз зарегистрировать пользователя в NDS и он получит доступ ко всем серверам сети.

3) В NetWare используется мощная и гибкая модель разграничения доступа. Система безопасности подключения к сети включает в себя: ограничения на срок действия и частоту смены пароля, запрет на повторное использование старых паролей, ограничение времени суток и адресов компьютеров, с которых пользователь может подключаться к сети, запрет одному и тому же пользователю на подключение к сети с нескольких машин одновременно. Система безопасности файловой системы позволяет для каждого файла и каталога назначить различным пользователям любую комбинацию следующих прав доступа: чтение, запись, создание, удаление, модификация (имени файла и его атрибутов), просмотр (содержимого каталога), изменение прав доступа, супервизор (полный набор всех прав). Аналогично регулируется доступ и к любым другим объектам NDS (права на просмотр, создание, удаление, переименование объектов, чтение, запись, сравнение и добавление их свойств, права супервизора). NetWare имеет также двухстороннюю систему аудита: внешние независимые аудиторы могут анализировать события в сети, не имея доступа к секретным данным, в то же время, администраторы сети не имеют доступа к данным аудита.

4) В NetWare 6.0 поддерживаются как традиционные тома (аналог логических дисков), так и тома NSS (Novell Storage Services). Традиционные тома обеспечивают надежную файловую систему, основанную на обработке транзакций (при сбое, файлы восстанавливаются в состояние "до сбоя"), сжатие файлов и систему зеркального отражения дисков (данные параллельно пишутся на два различных винчестера: при повреждении одного, информация будет считана с другого). Тома NSS могут иметь размер до 8 терабайт и хранить до 8 триллионов файлов. Доступ к томам NSS происходит гораздо быстрее, чем к традиционным томам. В качестве тома NSS может монтироваться CD-ROM и разделы DOS.

5) В NetWare 6.0 реализована распределенная система печати NDPS (Novell Distributed Print Services), которая была разработана совместно с компаниями Hewlett-Packard и Xerox и позволяет реализовать:

- двухсторонний обмен данными (компьютер имеет возможность передавать данные на принтер, и принтер имеет возможность передавать данные в компьютер).

- оповещение о событиях (принтер по сети имеет возможность оповестить технический персонал, например о том, что кончился тонер).

- автоматическая загрузка драйверов принтера, шрифтов и др. ресурсов на компьютеры, которым требуется производить распечатку документов.

6) В комплект поставки NetWare 6.0 входит мощный и простой в использовании Web-сервер FastTrack Server for NetWare, тесно интегрированный с NDS и поддерживающий большинство языков разработки приложений для Web. FastTrack Server призван заменить собой Novell Web Server, использовавшийся в предыдущих версиях NetWare.

7) В состав сервера NetWare 6.0 входит виртуальная машина Java, что позволяет запускать приложения и апплеты Java на сервере. Например, графическая утилита управления сервером ConsoleOne написана на языке Java.

### 3.1.2. Семейство ОС Windows 2000.

#### *3.1.2.1 Windows 2000 Server*

Включает основанные на открытых стандартах службы каталогов, Web, приложений, коммуникаций, файлов и печати, отличается высокой надежностью и простотой управления, поддерживает новейшее сетевое оборудование для интеграции с Интернетом. В Windows 2000 Server реализованы:

1. службы Internet Information Services 5.0 (IIS);
2. среда программирования Active Server Pages (ASP);
3. XML-интерпретатор;
4. архитектура DNA;
5. модель СОМ + ;
6. мультимедийные возможности;
7. поддержка приложений, взаимодействующих со службой каталогов;
8. Web-папки;
9. печать через Интернет.

Минимальные аппаратные требования Windows 2000 Server:

* Pentium-совместимый процессор с тактовой частотой не ниже 133 МГц — Windows 2000 Server поддерживает до 4 процессоров:
* 128 Мб ОЗУ (рекомендуется 256 Мб). Большее количество памяти значительно увеличивает быстродействие системы. Windows 2000 Server поддерживает ОЗУ объемом до 4 Гб;
* 2 Гб свободного дискового пространства — для установки Windows 2000 Server требуется около 1 Гб. Дополнительное место на диске необходимо для установки сетевых компонентов.

#### *3.1.2.2 Windows 2000 Advanced Server*

Эта ОС, по сути, представляет собой новую версию Windows NT Server 4.0 Enterprise Edition. Windows 2000 Advanced Server — идеальная система для работы с требовательными к ресурсам научными приложениями и приложениями электронной коммерции, где очень важны масштабируемость и высокая производительность[1]. Аппаратные требования для Windows 2000 Advanced Server не отличаются от требований для Windows 2000 Server, однако эта более мощная ОС включает дополнительные возможности:

* балансировку сетевой нагрузки;
* поддерживает ОЗУ объемом до 8 Гб на системах с Intel Page Address Extension (РАЕ);
* поддерживает до 8 процессоров.

#### *3.1.2.3 Windows 2000 Datacenter Server*

Это серверная ОС, еще больше расширяющая возможности Windows 2000 Advanced Server. Поддерживает до 32 процессоров и больший объем ОЗУ, чем любая другая ОС Windows 2000:

1. до 32 Гб для компьютеров с процессорами Alpha;
2. до 64 Гб для компьютеров с процессорами Intel.

Вопрос об установке Windows 2000 Datacenter Server следует рассматривать только в том случае, если вам требуется поддерживать системы *оперативной обработки транзакций* (online transaction processing, OLTP), крупные хранилища данных или предоставлять услуги Интернета[1].

### 3.1.3. ОС Windows Server 2003.

Семейство продуктов Windows Server 2003 берет все самое лучшее от технологии ОС Windows 2000 Server, упрощая при этом развертывание, управление и использование. В результате пользователь получает инфраструктуру высокой производительности, помогающую превратить сеть в стратегические активы организации.

Технология Windows Server 2003 содержит все функции, ожидаемые пользователями от серверной ОС Windows, используемой для выполнения ответственных задач, такие как безопасность, надежность, доступность и масштабируемость. Кроме того, корпорация Microsoft усовершенствовала и расширила серверную ОС Windows для того, чтобы организация могла оценить преимущества технологии Microsoft .NET, разработанной для связи людей, систем, устройств и обмена данными.

Windows Server 2003 является многозадачной операционной системой, способной централизовано или распределено управлять различными наборами ролей, в зависимости от потребностей пользователей. Некоторые из ролей сервера:

* файловый сервер и сервер печати;
* веб-сервер и веб-сервер приложений;
* почтовый сервер;
* сервер терминалов;
* сервер удаленного доступа/сервер виртуальной частной сети (VPN);
* служба каталогов, система доменных имен (DNS), сервер протокола динамической настройки узлов (DHCP) и служба Windows Internet Naming Service (WINS);
* сервер потокового мультимедиа-вещания.

### 3.1.4. ОС Unix, Linux

ОС Unix является старейшей сетевой операционной системой (создана в 1969г.) и по сегодняшний день использующейся в Internet. Существует множество клонов Unix — практически ничем не отличающихся друг от друга операционных систем разных производителей: FreeBSD, BSD Unix (университет Berkley), SunOS, Solaris (фирма Sun Microsystems), AIX (фирма IBM), HP-UX (фирмы Hewlet Packard), SCO (фирмы SCO) и др. Самым популярным клоном Unix пожалуй является FreeBSD, в основном из-за того, что ее исходные тексты распространяются свободно, что позволяет произвольно переделывать ОС "под себя", а также тестировать систему на отсутствие ошибок и "черного хода". В связи с этим, FreeBSD содержит гораздо меньше ошибок, чем коммерческие варианты Unix, т.к. отладкой и устранением ошибок занималась не одна компания, а все программистское сообщество.

К клонам Unix можно отнести и Linux, однако в последнее время он выделился в самостоятельную операционную систему и продолжает бурно развиваться. Существует множество дистрибутивов (пакетов установки) Linux различных фирм. Самые популярные из них — это Red Hat Linux (США) и Mandrake (Европа). Существуют также Slackware Linux, Corel Linux, Caldera OpenLinux, Debian Linux, SuSE Linux, Black Cat Linux, Connectiva Linux и др. Структура файловой системы, система разграничения доступа и основные команды в Linux и Unix сходны. С точки зрения пользователя, основным отличаем Linux от ранних версий Unix является удобный графический интерфейс, во многом сходный с интерфейсом Windows (особенно у графической рабочей среды Gnome), а основным преимуществом, по сравнению с Windows, -большая надежность и скорость работы, большая защищенность файловой системы (в том числе и от вирусов) и более профессиональные средства работы с локальной сетью и Internet. Для Linux существует и разрабатывается большое количество программного обеспечения: от офисного пакета Star Office и графического редактора Corel Draw, до мощных СУБД (DB2 фирмы IBM) и систем разработки программ на C++, Perl, Java и др. И хотя пока еще рано рекомендовать неопытному пользователю переходить на Linux (в основном из-за проблем с использованием русских шрифтов в приложениях — отсутствует единая прозрачная схема настройки), тем не менее, в будущем, Linux возможно займет значительное место в нише ОС для домашних компьютеров.

## 3.2. Обоснование выбора Операционной системы Windows 2000 Advanced Server .

В качестве операционной системы было решено использовать Windows 2000 Advanced Server. Эта версия Windows 2000 поддерживает работу с большим объемом оперативной памяти и большим количеством процессоров. Она включает в себя средства организации кластеров и механизмы распределения нагрузки. [13]

Таблица 3.2.1

*Характеристики различных версий Windows 2000.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Характеристика | Windows 2000 Professional | Windows 2000 Server | Windows 2000 Advanced Server | Windows 2000 Datacenter Server |
| Максимальный поддерживаемый объем памяти, Гбайт | 4 | 4 | 8 | 64 |
| Количество процессоров, поддерживаемое сразу же после установки | 2 | 4 | 8 | 32 |
| Максимальное допустимое количество процессоров | 10 | Ограничено возможностями аппаратной платформы | Ограничено возможностями аппаратной платформы | Ограничено возможностями аппаратной платформы |
| Служба каталога Active Directory | Клиент | Контроллер домена или член домена | Контроллер домена или член домена | Контроллер домена или член домена |
| Сервер Web | Одноранговые службы Web | Internet Information Server v. 5.0 | Internet Information Server v. 5.0 | Internet Information Server v. 5.0 |
| Сетевые службы | Нет | Да | Да | Да |
| DHCP, DNS, WINS, маршрутизация и служба удаленного доступа RAS | Нет | Да | Да | Да |
| Терминальные службы | Нет | Да | Да | Да |
| Службы слежения за транзакциями | Нет | Да | Да | Да |
| Отказоустойчивые дисковые тома (отражение дисков и RAID-5) | Нет | Да | Да | Да |
| Распределение сетевой нагрузки | Нет | Нет | Да | Да |
| Работа в кластере | Нет | Нет | Да | Да |

По сравнению с Windows NT 4.0 версия Windows 2000 Server обладает следую­щими новыми возможностями:

* Active Directory. Новая служба каталога, основанная на спецификациях Х.500 и заменяющая собой домены Windows NT 4.0. Служба Active Directory интегрирована с DNS, использует аутентификацию Kerberos, поддерживает наследуемые доверительные отношения и репликацию с несколькими глав­ными контроллерами домена.
* Улучшенная управляемость. Новая система включает в себя продуманный и последовательный интерфейс управления системой (Microsoft Management Console, MMC), поддержку групповой политики (Group Policy), средство ав­томатической установки Microsoft Installer, средства синхронизации папок в отключенном от сети состоянии, а также службы Telnet и Terminal Services (службы терминалов) для обеспечения удаленного администрирования.
* Улучшенная поддержка сети. Среди нововведений, связанных с работой в сети, следует упомянуть улучшенные службы DNS, WINS и DHCP, под­держку технологии Quality of Service (QoS), сжатие HTTP, защиту данных IP Security (IPSec), поддержку Asynchronous Transfer Mode (ATM), совместное использование канала связи с Интернетом (Internet Connection Sharing), под-дежку Virtual Private Network (VPN), а также службу маршрутизации и уда­ленного доступа Routing and Remote Access Service (RRAS).
* Улучшенная поддержка аппаратных устройств. Новая система включает в себя улучшенные драйверы существующего аппаратного обеспечения, а также цифровых видеодисков DVD (Digital Video Disks), устройств USB (Universal Serial Bus), новых сетевых адаптеров, сканеров, принтеров, моде­мов и других аппаратных устройств. В подавляющем большинстве случаев установка новых драйверов не требует перезагрузки системы. Если ранее пе­резагрузка системы требовалась приблизительно в пятидесяти случаях из ста, то теперь этот параметр снижен всего до семи случаев из ста.
* Управление системой долговременного хранения данных. Новая система включает в себя улучшенные механизмы хранения файлов, а также управле­ния данными, хранящимися на дисках и других устройствах долговременного хранения информации. Среди новых механизмов — квотирование дискового пространства, шифрование данных, управление сменными носителями ин­формации, контекстное индексирование и распределенная файловая система DPS (Distributed File System).
* Улучшенная производительность. Добавлена поддержка большего объема оперативной памяти, большего количества процессоров. Новая система более эффективно использует аппаратные ресурсы компьютера, а также позволяет следить за расходованием процессорного времени и управлять этим расходо­ванием.

Основные отличия Windows 2000 Advanced Server от Windows 2000 Server:

**Организация работы в кластере**. Кластеры используются для повышения степени надежности сетевой системы как единого целого. Если данные или сетевые приложения располагаются в кластере, состоящем из нескольких серверов, они будут доступны для пользователей даже при большой нагрузке на сеть или в случае, если один из серверов выйдет из строя. Windows 2000 поддерживает две основные разновидности кластерных технологий: распре­деление сетевой нагрузки (Network Load Balancing) и серверные кластеры. Эти кластерные технологии могут использоваться либо совместно, либо по отдельности.

**Поддержка многопроцессорных систем.** Каждая из версий Windows 2000 мо­жет поддерживать ограниченное количество процессоров, установленных на многопроцессорной системе. Windows 2000 Server поддерживает до четырех процессоров, Windows 2000 Advanced Server поддерживает до восьми процессо­ров, a Windows 2000 Datacenter Server будет поддерживать до 32 процессоров.

**Поддержка больших объемов оперативной памяти.** Windows 2000 Profes­sional и Windows 2000 Server поддерживают работу с оперативной памятью объемом до 4 Гбайт. Windows 2000 Advanced Server поддерживает работу с оперативной памятью объемом до 8 Гбайт (с использованием технологии Intel РАЕ — Physical Address Extention). Windows 2000 Datacenter Server может работать на компьютерах, оснащенных 64 Гбайт оперативной памяти (с использованием технологии Intel РАЕ).

Технология РАЕ позволяет установить на одном компьютере до 64 Гбайт опера­тивной памяти, использование которой осуществляется страницами по 4 Кбайт. Это значительно больше, чем позволял более ранний драйвер Intel PSE36.

В качестве операционной системы рабочих станции была выбрана - Windows 2000 Professional, она разработана для оснащения настоль­ных рабочих станций корпоративных пользователей. Она оптимизирована для выполнения функций сетевого клиента и управления работой персональ­ной рабочей станции.

Это настольная ОС, расширяющая возможности Windows NT в области безопасности и отказоустойчивости, она унаследовала от Windows 98 легкость в управлении, поддержку множества устройств и РnР. Windows 2000 Professional можно установить путем обновления любой ОС, начиная с Windows NT Workstation 3.51 и до Windows 98. Минимальные системные требования Windows 2000 Professional:

* Pentium-совместимый процессор с тактовой частотой не ниже 133 МГц – Windows 2000 Professional поддерживает до двух процессоров;
* 64 Мб ОЗУ — большее количество памяти повышает быстродействие системы;
* жесткий диск объемом не менее 2 Гб — для установки самой ОС Windows 2000 Professional на вашем жестком диске должно быть свободно минимум 650 Мб. [2]

# 4. Планирование структуры сети

Компьютерная сеть - это несколько компьютеров в пределах ограниченной территории (находящихся в одном помещении, в одном или нескольких близко расположенных зданиях) и подключенных к единых линиям связи. Сегодня большинство компьютерных сетей – это локальные компьютерные сети (Local-Area Network), которые размещаются внутри одного конторского здания и основанные на компьютерной модели клиент/сервер. Сетевое соединение состоит из двух участвующих в связи компьютеров и пути между ними. Можно создать сеть, используя беспроводные технологии, но пока это не распространено. [7]

В модели клиент/сервер связь по сети делится на две области: сторону клиента и сторону сервера. По определению, клиент запрашивает информацию или услуги из сервера. Сервер в свою очередь, обслуживает запросы клиента. Часто каждая сторона в модели клиент/сервер может выполнять функции, как сервера, так и клиента. При создании компьютерной сети необходимо выбрать различные компоненты, определяющие, какое программное обеспечение и оборудование вы сможете использовать, формируя свою корпоративную сеть. Компьютерная сеть – это неотъемлемая часть современной деловой инфраструктуры, а корпоративная сеть – лишь одно из используемых в ней приложений и, соответственно, не должна быть единственным фактором, определяющим выбор компонентов сети. Необходимые для Intranet компоненты должны стать дополнением к имеющейся сети, не приводя к существенному изменению ее архитектур. [6]

## 4.1. Способ управления сетью

Каждая организация формулирует собственные требования к конфигурации сети, определяемые характером решаемых задач. В первую очередь необходимо определить, сколько человек будут работать в сети. От этого решения, по существу, будут зависеть все последующие этапы создания сети.

Количество рабочих станций напрямую зависит от предполагаемого числа сотрудников. Другим фактором является иерархия компании. Для фирмы с горизонтальной структурой, где все сотрудники должны иметь доступ к данным друг друга, оптимальным решением является простая одноранговая сеть. [2]

Фирме, построенной по принципу вертикальной структуры, в которой точно известно, какой сотрудник и к какой информации должен иметь доступ, следует ориентироваться на более дорогой вариант сети – с выделенным сервером. Только в такой сети существует возможность администрирования прав доступа (рис. 4.1).

Количество рабочих станций в сети

5 и более рабочих станций

От 3 до 5 рабочих станций

Вертикальная структура предприятия

Горизонтальная структура предприятия

Вертикальная структура предприятия

Горизонтальная структура предприятия

Требуется установка сервера

Возможно использование одноранговой сети

Желательна установка сервера

Требуется установка сервера

Рис. 4.1 Выбор типа сети.

В данном случае на предприятии имеется 30 рабочих станции, которые и требуется объединить в корпоративную сеть. Причем они объединены в следующие группы:

* директор предприятия – 1 рабочая станция;
* отдел прямого подчинения - 2 рабочих станции;
* секретарь – 1 рабочая станция;
* отделения 1, 2 и 3 2-го отдела по 3, 3 и 4 рабочих станции соответственно;
* отделения 4 и 5 3-го отдела по 4 и 4 рабочих станции;
* отделение 6 4-го отдела – 4 рабочих станции.

Следуя из схемы выбора типа сети, можно решить, что в данном случае требуется установка сервера, так как мы имеем вертикальную структуру предприятия, то есть разграниченный доступ к информации.

Одним из главных этапов планирования является создание предварительной схемы. При этом в зависимости от типа сети возникает вопрос об ограничении длины кабельного сегмента. Это может быть несущественно для небольшого офиса, однако если сеть охватывает несколько этажей здания, проблема предстает в совершенно ином свете. В таком случае необходима установка дополнительных репитеров (repeater).

В ситуации с предприятием вся сеть будет располагаться на одном этаже, и расстояние между сегментами сети не столь велико, чтобы требовалось использование репитеров.

## 4.2. Размещение сервера

В отличие от установки одноранговой сети, при построении ЛВС с сервером возникает еще один вопрос - где лучше всего установить сервер.

На выбор места влияет несколько факторов:

* из-за высокого уровня шума сервер желательно установить отдельно от остальных рабочих станций;
* необходимо обеспечить постоянный доступ к серверу для технического обслуживания;
* по соображениям защиты информации требуется ограничить доступ к серверу;

|  |
| --- |
|  |

Рис. 4.2. План помещения.

Сервер расположен в комнате сетевого администратора, так как только это помещение удовлетворяет требованиям, то есть уровень шума в помещении минимален, помещение изолированно от других, следовательно, доступ к серверу будет ограничен.

Сетевой администратор сможет постоянно следить за работой сервера и осуществлять обслуживание сервера, так как при установке сервера.

## 4.3. Сетевая архитектура

Сетевая архитектура - это сочетание топологии, метода доступа, стандартов, необходимых для создания работоспособной сети.

Выбор топологии определяется, в частности, планировкой помещения, в котором разворачивается ЛВС. Кроме того, большое значение имеют затраты на приобретение и установку сетевого оборудования, что является важным вопросом для фирмы, разброс цен здесь также достаточно велик.

Топология типа «звезда» представляет собой более производительную структуру, каждый компьютер, в том числе и сервер, соединяется отдельным сегментом кабеля с центральным концентратором (HAB).

Основным преимуществом такой сети является её устойчивость к сбоям, возникающим вследствие неполадок на отдельных ПК или из-за повреждения сетевого кабеля. [12]

|  |
| --- |
|  |

Рис. 4.3 Топология сети предприятия.

Важнейшей характеристикой обмена информацией в локальных сетях являются так называемые методы доступа (access methods), регламентирующие порядок, в котором рабочая станция получает доступ к сетевым ресурсам и может обмениваться данными.

За аббревиатурой CSMA/CD скрывается английское выражение «Carrier Sense Multiple Access with Collision Detection » (коллективный доступ с контролем несущей и обнаружением коллизий). С помощью данного метода все компьютеры получают равноправный доступ в сеть. Каждая рабочая станция перед началом передачи данных проверяет, свободен ли канал. По окончании передачи каждая рабочая станция проверяет, достиг ли адресата отправленный пакет данных. Если ответ отрицательный, узел производит повторный цикл передачи/контроля приема данных и так до тех пор, пока не получит сообщение об успешном приеме информации адресатом. [6]

Так как этот метод хорошо зарекомендовал себя именно в малых и средних сетях, для предприятия данный метод подойдет. К тому же сетевая архитектура Ethernet, которую и будет использовать сеть предприятия, использует именно этот метод доступа.

Спецификацию Ethernet в конце семидесятых годов предложила компания Xerox Corporation. Позднее к этому проекту присоединились компании Digital Equipment Corporation (DEC) и Intel Corporation. В 1982 году была опубликована спецификация на Ethernet версии 2.0. На базе Ethernet институтом IEEE был разработан стандарт IEEE 802.3. [12]

В настоящее время технология, применяющая кабель на основе витой пары (10Base – T), является наиболее популярной. Такой кабель не вызывает трудностей при прокладке.

Сеть на основе витой пары, в отличие от тонкого и толстого коаксиала, строится по топологии звезда. Чтобы построить сеть по звездообразной топологии, требуется большее количество кабеля (но цена витой пары не велика). Подобная схема имеет и неоценимое преимущество – высокую отказоустойчивость. Выход из строя одной или нескольких рабочих станций не приводит к отказу всей системы. Правда если из строя выйдет хаб, его отказ затронет все подключенные через него устройства.

Еще одним преимуществом данного варианта является простота расширения сети, поскольку при использовании дополнительных хабов (до четырех последовательно) появляется возможность подключения большого количества рабочих станций (до 1024). При применении неэкранированной витой пары (UTP) длина сегмента между концентратором и рабочей станцией не должна превышать 100 метров, чего не наблюдается в предприятии.

## 4.4. Сетевые ресурсы

Следующим важным аспектом планирования сети является совместное использование сетевых ресурсов (принтеров, факсов, модемов).

Перечисленные ресурсы могут использоваться как в одноранговых сетях, так и в сетях с выделенным сервером. Однако в случае одноранговой сети сразу выявляются её недостатки. Чтобы работать с перечисленными компонентами, их нужно установить на рабочую станцию или подключить к ней периферийные устройства. При отключении этой станции все компоненты и соответствующие службы становятся недоступными для коллективного пользования. [2]

В сетях с сервером такой компьютер существует по определению. Сетевой сервер никогда не выключается, если не считать коротких остановок для технического обслуживания. Таким образом, обеспечивается круглосуточный доступ рабочих станций к сетевой периферии.

На предприятии имеется десять принтеров: в каждом обособленном помещении. Администрация пошла на расходы для создания максимально комфортных условий работы коллектива.

Теперь вопрос подключения принтера к ЛВС. Для этого существует несколько способов.

1.Подключение к рабочей станции.

Принтер подключается к той рабочей станции, которая находиться к нему ближе всего, в результате чего данная рабочая станция становится сервером печати. Недостаток такого подключения в том, что при выполнении заданий на печать производительность рабочей станции на некоторое время снижается, что отрицательно скажется на работе прикладных программ при интенсивном использовании принтера. Кроме того, если машина будет выключена, сервер печати станет недоступным для других узлов.

2.Прямое подключение к серверу.

Принтер подключается к параллельному порту сервера с помощью специального кабеля. В этом случае он постоянно доступен для всех рабочих станций. Недостаток подобного решения обусловлен ограничением в длине принтерного кабеля, обеспечивающего корректную передачу данных. Хотя кабель можно протянуть на 10 и более метров, его следует прокладывать в коробах или в перекрытиях, что повысит расходы на организацию сети.

3. Подключение к сети через специальный сетевой интерфейс.

Принтер оборудуется сетевым интерфейсом и подключается к сети как рабочая станция. Интерфейсная карта работает как сетевой адаптер, а принтер регистрируется на сервере как узел ЛВС. Программное обеспечение сервера осуществляет передачу заданий на печать по сети непосредственно на подключенный сетевой принтер.

В сетях с шинной топологией сетевой принтер, как и рабочие станции соединяется с сетевым кабелем при помощи Т-коннектора, а при использовании «звезды» - через концентратор.

Интерфейсную карту можно установить в большинство принтеров, но её стоимость довольно высока.

4. Подключение к выделенному серверу печати.

Альтернативой третьему варианту является использование специализированных серверов печати. Такой сервер представляет собой сетевой интерфейс, скомпонованный в отдельном корпусе, с одним или несколькими разъемами (портами) для подключения принтеров. Однако в данном случае использование сервера печати является непрактичным.

В нашем случае в связи с нерентабельностью установки специального сетевого принтера, покупкой отдельной интерфейсной карты для принтера самым подходящим способом подключения сетевого принтера является подключение к рабочей станции. На это решение повлиял ещё и тот факт, что принтеры расположены около тех рабочих станций, потребность которых в принтере наибольшая. [10]

# 5. Организация сети на основе Windows 2000.

## 5.1. Служба каталогов Windows 2000

Безусловно, наиболее значимое изменение, по сравнению с Windows NT 4, это включение в Windows 2000 важной новой службы – Active Directory. Active Directory – это «родная» служба каталогов для Windows 2000. В NT 4 домен был очень похож на удаленный остров, с которым мы могли соединиться только используя механизм доверительных отношений. Active Directory – полнофункциональная служба каталогов.

Каталог может хранить различную информацию, относящуюся к пользователям, группам, компьютерам, принтерам, общим ресурсам и так далее – все это называется **объектами**.

Каталог хранит также информацию о самом объекте, или его свойства – **атрибутамы**. Например, атрибутами, хранимыми в каталоге о пользователе, может быть имя его руководителя, номер телефона, адрес, имя для входа в систему, пароль, группы, в которые он входит и многое другое. [4]

### 5.1.1. Наименование объектов

Active Directory использует Lightweight Directory Access Protocol (LDAP) – простой протокол доступа к каталогам, как главный протокол доступа. LDAP действует поверх TCP/IP и определяет способы обращения и доступа к объектам между клиентом и сервером Active Directory. В LDAP каждый объект имеет свое особенное Distinguished Name (отличительное имя), и это имя отличает его от других объектов Active Directory, а также подсказывает нам, где данный объект расположен. Два главных составных части отличительного имени – это CN (common name) – общее имя и DC (domain component) – доменная составляющая. Общее имя определяет объект или контейнер, в котором этот объект находится, в то время как доменный компонент определяет домен, в котором объект находится. Например, отличительное имя может быть следующим:

**CN=Peter Ivanoff, CN=Users, DC=firma, DC=ru**

В этом примере у нас есть пользователь Peter Ivanoff, который находится внутри контейнера, называемого Users, в домене firma, который является поддоменом .ru. Отличительное имя объекта должно быть уникальным внутри леса Active Directory.

В то время как отличительное имя дает нам полную информацию о расположении объекта, relative distinguished name (относительное отличительное имя) определяет объект внутри его родительского контейнера. Например, если я осуществляю поиск внутри контейнера Users, относительное отличительное имя объекта, который я ищу, может быть Peter Ivanoff.

Когда пользователь входит в домен, расположенный в Active Directory, у него может быть два типа имени. Первое из них – традиционное NetBIOS -имя. В Windows 2000 на него ссылаются как на downlevel logon name (имя регистрации в ранних версиях Windows). Этот тип имени существует для совместимости с ранними версиями Windows, процесс входа в которые был основан на использовании имен NetBIOS (такие OS как NT 4, Windows 9x и так далее). Когда вы используете downlevel logon name (на вкладке свойств –«имя входа пользователя пред-Windows 2000») для входа, пользователь должен ввести имя пользователя, пароль и выбрать соответствующий домен, в который он собирается входить. Второе имя – и это новинка в Windows 2000 – это возможность входа в систему с использованием того, что называется User Principal Name (основное имя пользователя) или UPN. Основное имя пользователя имеет следующий формат – user@domain.com (на вкладке свойств пользователя это называется – User logon name (имя входа пользователя)). Если это соглашение действует, то пользователю не нужно определять домен, в который он хочет войти. Фактически, когда для входа в Windows 2000используется UPN, доменная часть окна имени для входа в систему закрашена серым. Пример этих двух типов имен показан на вкладке свойств учетной записи пользователя Active Directory:

|  |
| --- |
|  |

Рис. 5.1. Active Directory

### 5.1.2. Логическая структура Active Directory

Логическая структура Active Directory зависит от нужд вашей организации. Логические элементы Active Directory это леса, деревья, домены и OU.

#### *5.1.2.1. Домены*

Домен в Windows 2000 очень напоминает домен в Windows NT. Для различных намерений и целей, домен является логической группой пользователей и компьютеров (объектов), которые связаны как единица для администрирования и репликации. Прежде всего домен – это административная единица. Следовательно, администратор этого домена может его администрировать и для этого не нужен никто другой. Кроме того, все контроллеры одного домена должны осуществлять репликацию друг с другом.

В Windows 2000 домены именуются в соответствии с соглашением об именовании DNS, а не именовании NetBIOS. Примером имени домена в Active Directory может быть 2000trainers.com. В Windows NT имели ограничения по величине, до которой они могли увеличиваться и этот размер ограничивался допустимым размером базы данных SAM (40 Мб или около того). Поэтому приходилось создавать множества доменов в компании, в которой действовали тысячи пользователей и компьютеров. Теперь же множество доменов не являются необходимостью в подобном сценарии под Windows 2000, так как Active Directory может вместить в себя многие миллионы объектов. Учетные записи пользователей в Windows 2000 существуют так же как и в Windows NT. Active Directory также позволяет иметь множество доменов, формируя структуры, которые называются деревьями и лесами. [4]

#### *5.1.2.2 Дерево*

В Windows 2000, несколько доменов может все же потребоваться, особенно в больших организациях, которые продолжают требовать надежного контроля над их средой, их индивидуальностью (как в случае различных организационных единиц для ведения бизнеса) и особого административного контроля. В Active Directory набор доменов может создаваться в порядке, напоминающем структуру дерева. В этом случае «дочерний» домен наследует свое имя от «родительского» домена:

|  |
| --- |
| firma.ru  filial1.firma.ru  filial2.firma.ru |

Рис. 5.2. Домены

Каждый домен в дереве является отдельной и явно выраженной административной единицей, так же как и границей для целей репликации. То есть, если вы создали учетную запись пользователя в домене filial1.firma.ru, то эта учетная запись, существующая на контроллере домена, будет реплицирована на все контроллеры домена filial2.firma.ru.

Каждый новый «дочерний» домен имеет transitive (транзитивные) двунаправленные доверительные отношения с «родительским» доменом. Это достигается автоматически в Active Directory и позволяет пользователям из одного домена дерева иметь доступ к ресурсам в другом. Даже не имея прямых доверительных отношений, пользователи в filial1 могут получать доступ к ресурсам (для чего у них должны быть соответствующие разрешения) в filial2 и наоборот, к тому же доверительные отношения транзитивны (filial1 доверяет своему «родительскому» домену firma , который в свою очередь «доверяет» filial2 – таким образом filial1 доверяет filial2 и наоборот).

Дерево, в общих чертах, можно определить как набор доменов, которые связаны отношениями «дочерний»/«родительский» и поддерживают связанное пространство имен. [4]

#### *5.1.2.3 Лес*

Лес – это термин, применяемый для описания совокупности Active Directory деревьев. Каждое дерево в лесе имеет собственное отдельное пространство имен. Например, давайте предположим, что наша фирма владеет еще одной более мелкой, называемой ЧП Сидоров. Чтобы ЧП Сидоров имело свое собственное отдельное пространство имен, я могу достичь этого объединив деревья и сформировать лес, как показано ниже:

|  |
| --- |
| firma.ru  filial1.firma.ru  filial2.firma.ru  Sidoroff.ru |

Рис. 5.3. Лес

Домен Sidoroff.ru является частью леса, так же как и firma.ru, но по-прежнему остается доменом и может иметь собственное дерево. Заметьте, что здесь существуют транзитивные доверительные отношения между «корневыми» доменами каждого дерева в лесу – это позволит пользователям домена acmeplunbing.com получать доступ к ресурсам в дереве firma.ru и наоборот, в то же время поддерживает проверку подлинности в собственном домене.

Первый домен, созданный в лесу, рассматривается как «корень» леса. Одна из самых важных особенностей леса – это то, что каждый отдельный домен поддерживает общую схему – определения для различных объектов и связанных с ними атрибутов, которые созданы в лесу. Важно осознать, что лес может быть создан из одного дерева, которое содержит всего один домен. Это будет маленький лес, но формально это будет лес. [4]

#### *5.1.2.4 Организационные единицы*

Организационные единицы (обычно называемые OU) – это контейнеры внутри Active Directory которые создаются для объединения объектов в целях делегирования административных прав и применения групповых политик в домене. OU могут быть созданы для организации объектов несколькими путями, в соответствии с их функциями, местоположением, ресурсами и так далее. Примером объектов, которые могут быть объединены в OU могут служить учетные записи пользователей, компьютеров, групп и т.д. Рисунок 5.1.3 показывает пример OU, основанной на местоположении пользователей и ресурсов:

|  |
| --- |
|  |

Рис. 5.4. Организационные единицы.

OU может содержать только объекты из того домена, в котором они расположены. Также заметьте, что структура OU может широко варьироваться от компании к компании. Она разрабатывается с целью облегчить администрирование ресурсов и применения групповых политик. В то время как полный административный контроль может быть дан (делегирован) пользователю через OU, для больших организаций становиться возможным иметь только один домен, в котором каждая структура будет имеет собственный контроль только над своей OU. [1]

### 5.1.3. Физическая структура

Физическая структура Active Directory связана с двумя главными типами объектов – сайтами и контроллерами доменов.

#### *5.1.3.1 Сайты*

В отличии от NT 4, в Windows 2000 Active Directory предусматривает концепцию физического местоположения внутри структуры. В Active Directory сайт – это совокупность подсетей TCP/IP, между которыми существует высокоскоростное соединение. Хотя «высокоскоростное» - это относительное понятие, обычно под этим подразумевается соединение на скоростях, соответствующих LAN – соединениям. Вы определяете сайт в Active Directory для контроля репликации, аутентификации и местоположения служб. Как только сайт будет создан, компьютеры клиентов будут пытаться аутентифицироваться на контроллере домена, который находится на данном сайте, вместо того, чтобы посылать запросы по WAN (глобальной сети).

Сайты также позволяют вам контролировать, когда репликация может происходить между контроллерами доменов. Например, в NT 4, все BDC получают данные от PDC в процессе репликации, используя 5-минутный интервал уведомления об изменениях. Так как в NT не было предусмотрено простого пути для контроля репликации между физическими местоположениями (это можно сделать, используя специальные скрипты для регистра), трафик репликации может перегрузить линии и снизить производительность сети. Если же вы определите сайт в Active Directory, вы можете также определить время и дни, в которые репликация между сайтами должна происходить, как часто она должна происходить, и преимущественные пути для ее прохождения. Вы должны заметить, однако, что по умолчанию существует только один сайт, и пока вы не создадите другие, репликация будет происходить, как и раньше, каждый 5-минутный интервал уведомления об изменениях. Также важно отметить, что сайты – это другой элемент, который позволяет большим компаниям иметь только один домен. Так как не существует соотношения между логической и физической структурой Active Directory, вы можете иметь один домен и сотню сайтов. Возможность контролировать трафик репликации – одно из наибольших преимуществ управляемости Active Directory.

#### *5.1.3.2 Контроллеры доменов*

Домена не может существовать без по крайней мере одного контроллера домена, где храниться база данных Active Directory. В отличие от Windows NT, где была только одна копия базы, позволяющая делать запись (хранящаяся на PDC; копии, хранящиеся на BDC имели атрибут «только для чтения»), в Windows 2000 каждый контроллер домена имеет копию базы данных Active Directory, в которую можно производить запись. Поэтому все контроллеры домена в среде Active Directory достаточно равноправны. Однако, это усложняет картину, так как теперь каждый контроллер домена может делать записи в базу данных. Как и в NT 4, должно быть как минимум два контроллера в домене для целей избыточности, а, как правило, и гораздо больше, в зависимости от размера организации. [4]

Создаете контроллер домена в Windows 2000, при помощи Installation Wizard (мастер установки Active Directory) – **dcpromo.exe**. Этот инструмент не только позволяет создавать новые контроллеры домена, и новые домены, деревья и леса. Он позволяет также понижать контроллер домена до рядового сервера, если возникнет такая необходимость.

|  |
| --- |
|  |

Рис. 5.5. Installation Wizard

После того, как контроллер домена создан, он хранит копию базы данных Active Directory (**ntds.dit**) и может проводить аутентификацию пользователей домена. База данных Active Directory состоит из того, что принято называть тремя разделами, как показано на рисунке 5.1.5.

|  |
| --- |
|  |

Рис. 5.6. База данных Active Directory.

Раздел «домен» реплицируется между контроллерами только внутри одного домена, в то время как разделы «конфигурация» и «схема» реплицируются в каждый из доменов, расположенных в лесу. Некоторые из контроллеров домена отличаются от других специальными ролями, которые они выполняют:

**Global Catalog Server** (сервер Глобального Каталога) – сервер Глобального Каталога – это контроллер домена, который знает о каждом единичном объекте, который существует в Active Directory, в каждом из доменов. Однако, он сохраняет только часть атрибутов каждого объекта, которые считаются наиболее важными. По умолчанию только один контроллер домена во всем лесу выполняет эту роль – первый контроллер домена, созданный в лесу. Большее число серверов Глобального Каталога может (и должно) быть создано в лесу. Когда контроллер домена действует как сервер Глобального Каталога он хранит четвертый раздел, как часть базы данных Active Directory – раздел Глобального Каталога.

Помимо роли сервера Глобального Каталога, контроллеры домена могут выполнять еще пять специальных ролей, называемых Operations Masters (основные контроллеры операций). Они перечислены ниже:

**Schema Master** (хозяин схемы) – в лесу только один контроллер домена может выполнять эту роль. Schema Master поддерживает схему Active Directory и поддерживает копию схемы, доступную для записи. По умолчанию первый контроллер домена, созданный в корневом домене леса, выполняет эту роль.

**Domain Naming Master** (Хозяин именования доменов) – этот контроллер домена отслеживает домены, которые создаются и удаляются из леса, поддерживая целостность структуры леса, если какие-либо изменения имеют место. В лесу существует только один Domain Naming Master и, по умолчанию, эту роль выполняет первый контроллер, созданный в корневом домене леса.

**PDC Emulator** (хозяин PDC) – эта роль существует по паре причин, одна из которых – обратная совместимость с NT 4 контроллерами. Когда домен повышается до Windows 2000, первая система, которая подвергается модернизации – это PDC (главный контроллер домена), и этот новый контроллер домена Windows 2000 эмулирует (имитирует) старый PDC для оставшихся BDC (резервных контроллеров домена), работающих под Windows NT. PDC Emulator отслеживает изменения паролей и выступает «арбитром» перед тем, как пароль может быть отвергнут системой. По умолчанию клиенты предыдущих Windows OS, таких как Windows 9x и NT продолжают изменять свои пароли на PDC Emulator (до тех пор, пока на систему не будет установлен клиент Active Directory). Один контроллер в каждом домене выполняет роль PDC Emulator, по умолчанию, это первый контроллер созданный в домене.

**Relative Identifier (RID) Master** (Хозяин RID (relative identificator)) – в NT 4, PDC отвечает за создание всех SID (security identificator), то есть отвечает за создание всех объектов безопасности («пользователь», «группа», «компьютер»). В Windows 2000 каждый контроллер домена может создавать объекты безопасности. На самом деле SID состоит из двух частей - SID (который определяет домен) и RID (который определяет уникальный объект внутри домена).Для того, чтобы быть уверенным, что SID уникален, один контроллер в каждом домене выполняет роль RID Master, отвечающего за создание доменного пула RID, и размещения этих RID на других контроллерах в домене. Это позволяет быть уверенным, что не произойдет дублирования объектов SID. В каждом домене Active Directory действует один RID Master, по умолчанию, это первый контроллер, созданный в домене.

**Infrastructure Master** (Хозяин инфраструктуры) - Infrastructure Master отслеживает информацию о том, какие пользователи (из других доменов) являются членами той или иной группы данного домена и все изменения, которые имеют место. Это позволяет быть уверенным в непротиворечивости участия пользователей в группах в Active Directory. Каждый домен в Active Directory имеет одного Infrastructure Master, по умолчанию, это первый контроллер, созданный в домене. [1]

## 5.2. Служба DHCP.

Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста) является базовой сетевой службой, предлагаемой Windows 2000 для динамического распределения IP-адресов и связанной с ними информации клиентам, использующим TCP/IP. Хотя функции, выполняемые DHCP в Windows 2000 во многом похожи на те, что были в Windows NT, некоторое количество несущественных отличий.

DHCP — развитие протокола ВООТР (RFC 951 и 1084), позволявшего динамически назначать IP-адреса (в дополнение к удаленной загрузке бездисковых станций). При этом DHCP предоставляет все данные для настройки стека протоколов TCP/IP и дополнительные данные для функционирования определенных серверов (Приложение 2).

*Область DHCP*. Область (scope) DHCP — административная группа, идентифицирующая полные последовательные диапазоны возможных IP-адресов для всех клиентов DHCP в физической подсети. Области определяют логическую подсеть, для которой должны предоставляться услуги DHCP, и позволяют серверу задавать параметры конфигурации, выдаваемые всем клиентам DHCP в подсети. Область должна быть определена прежде, чем клиенты DHCP смогут использовать сервер DHCP для динамической конфигурации TCP/IP.

*Пул адресов*. Если определена область DHCP и заданы диапазоны исключения, то оставшаяся часть адресов называется пулом доступных адресов (address pool) (в пределах области). Эти адреса могут быть динамически назначены клиентам DHCP в сети.

*Диапазоны исключения*. Диапазон исключения (exclusion range) — ограниченная последовательность IP-адресов в пределах области, которые должны быть исключены из предоставления службой DHCP.

*Резервирование*. Резервирование (reservation) позволяет назначить клиенту постоянный адрес и гарантировать, что указанное устройство в подсети может всегда использовать один и тот же IP-адрес.

*Суперобласти.* Это понятие, используемое в Диспетчере DHCP, которое задает множество областей, сгруппированных в отдельный административный объект — суперобласть (superscope). Суперобласти полезны для решения различных задач службы DHCP.

*Арендные договоры****.*** Арендный договор (lease) — отрезок времени, определяющий период, во время которого клиентский компьютер может использовать назначенный IP-адрес. При выдаче арендного договора он становится активным. В момент половины срока действия арендного договора клиент должен возобновить назначение адреса, обратившись к серверу повторно. Продолжительность арендного договора влияет на частоту обновления арендных договоров (интенсивность обращений к серверу).

*Опции DHCP* — дополнительные параметры настройки клиентов, которые сервер DHCP может назначать при обслуживании арендных договоров клиентов DHCP. Например, IP-адреса маршрутизатора или шлюза по умолчанию, серверов WINS или серверов DNS обычно предоставляются для каждой области или глобально для всех областей, управляемых сервером DHCP. Кроме стандартных опций, сервер DHCP Microsoft позволяет определять и добавлять пользовательские опции. [4]

Служба DHCP в Windows 2000 состоит из трех основных компонентов.

***Серверы DHCP.*** В состав сервера DHCP входит оснастка DHCP — удобный в работе графический инструмент, который позволяет администратору настраивать конфигурации для клиентов DHCP. Сервер DHCP также содержит базу данных для назначения IP-адресов и других параметров настройки. Сервер DHCP поддерживает более 30 опций DHCP согласно RFC 2132. Параметры конфигурации TCP/IP, которые могут быть назначены сервером DHCP, включают: IP-адрес для каждого сетевого адаптера на клиентском компьютере, маску подсети, шлюзы по умолчанию, дополнительные параметры конфигурации, например, IP-адрес сервера DNS или WINS. Один или более компьютеров в сети должны работать под управлением Windows 2000 Server с протоколом TCP/IP и установленным сервером DHCP. Если служба сервера DHCP установлена на компьютере, то сразу после задания и активизации областей автоматически создается база данных DHCP.

***Клиенты DHCP.*** Клиентами сервера DHCP из состава Windows 2000 могут быть компьютеры, работающие на любой платформе. Компьютеры под управлением ОС производства Microsoft могут действовать как клиенты DHCP: Windows NT Server/Workstation (все версии), Windows 98/95, Windows for Workgroups 3.11 (с установленным 32-разрядным протоколом TCP/IP), Microsoft Network Client 3.0 for MS-DOS (с установленным драйвером реального режима), LAN Manager версии 2.2с.

Работа протоколов ВООТР и DHCP основана на механизмах широковещания. Маршрутизаторы обычно по умолчанию не ретранслируют широковещательные посылки, поэтому передача таких посылок выполняется агентом ретрансляции. Агент ретрансляции DHCP — это маршрутизатор, либо хост, который слушает широковещательные сообщения DHCP/BOOTP и переадресовывает их на заданный сервер (серверы) DHCP. Использование агентов ретрансляции избавляет от необходимости устанавливать сервер DHCP в каждом физическом сегменте сети. Агент не только обслуживает прямые локальные запросы клиента DHCP и перенаправляет их на удаленные серверы DHCP, но также возвращает ответы удаленных серверов DHCP клиентам DHCP.

Администратор может отменить параметры динамической настройки, настроив их вручную. Любая информация, вручную введенная на клиенте, отменяет параметры динамической настройки.

### 5.2.1. Настройка службы DHCP.

Служба сервера DHCP устанавливается автоматически на сервер Windows 2000, но не является сконфигурированной (и даже может быть отключена) без дополнительной настройки. Она может быть удалена и добавлена в случае необходимости, посредством использования вкладки Add/Remove Windows Components программы Add/Remove Programs в Control Panel (в разделе Networking Services). После установки, сервер DHCP настраивается при помощи оснастки DHCP ММС, которая находится в Administrative Tools. Если сервер Windows 2000 является частью рабочей группы или домена, основанного на Windows 2000, то сервер DHCP будет запущен по умолчанию, но необходимо будет вручную настроить области используемых IP-адресов для распределения их службой DHCP. Если DHCP установлена на систему, являющуюся частью домена Windows 2000, то служба DHCP не сможет быть запущена до тех пор, пока сервер DHCP не будет авторизован в Active Directory. Авторизация сервера DHCP в Active Directory может быть осуществлена только членом группы Enterprise Admins. Эта особенность используется как контрольный механизм, позволяющий избежать такой проблемы, как установка незарегистрированных серверов DHCP (пользователями с административными привилегиями), могущих создать проблемы с настройкой TCP/IP сетей (так как клиент получает IP-адрес от первого же сервера DHCP, который отвечает на его запрос).

В Active Directory домене (Windows 2000), только авторизованные Windows 2000 сервера DHCP могут выполнять распределение IP-адресов. В Windows NT 4.0 сервер DHCP может (и будет) распределять адреса и не попадет под действие авторизации. Однако если другой администратор попытается установить Windows 2000 сервер DHCP и запустить службу без предварительной авторизации, то сервер осуществит запрос AD и не запустит службу, если не найдет подтверждения ее авторизации в сети. Неавторизованный сервер DHCP появляется в консоли DHCP с указывающей вниз красной стрелкой (которая может обозначать также, что служба не запущена или область адресов не настроена), как показано на рисунке 5.7.

|  |
| --- |
|  |

Рис. 5.7. Консоль DHCP.

Для авторизации DHCP сервер, нужно щелкнуть правой кнопкой мыши на значке сервера и выбрать опцию Authorize (авторизовать) из появившегося меню. Для управления авторизованным DHCP сервером (включая добавление или удаление авторизованных серверов), щелкните правой кнопкой мыши на иконке DHCP и выберите Manage Authorized Servers (управление авторизованными серверами), как показано на рисунке 5.8:

|  |
| --- |
|  |

Рис. 5.8 Рис. Управление авторизованными серверами

Заметьте, что сервер DHCP не будет выполнять никаких функций, до тех пор, пока вы не сконфигурируете область адресов – набор настроек, которые будут распределяться группе клиентов. Как и большинство других вещей в Windows 2000, процесс создания области осуществляется с применением соответствующего мастера. Для создания области адресов, щелкните правой кнопкой мыши на значке сервера DHCP и выберите опцию New Score (новая область). Мастер проведет вас через длинный процесс, включающий в себя настройку допустимого диапазона IP-адресов, маски подсети и таких опций, как адрес шлюза по умолчанию (маршрутизатора), используемых серверов DNS и так далее. После того, как область будет настроена, она будет продолжать нуждаться в активизации (правый щелчок мыши и выбор Activate (активизировать)). Каждая область включает в себя: набор адресов, активные выделенные адреса, резервирование и свойства области, как показано на рисунке 5.9 (свойства области выделены):

|  |
| --- |
|  |

Рис. 5.9. Консоль DHCP.

После того, как сервер авторизован и область настроена, стрелка на иконке сервера меняется на зеленую и теперь указывает вверх.

Области в Windows 2000 Advanced Server:

- Области могут быть собраны или объединены для создания суперобластей. Они позволяют распределять диапазоны IP-адресов, которые не примыкают друг к другу, но расположены на одной подсети.

- Для изменения маски подсети, связанной с областью, необходимо будет удалить область и создать ее заново.

- Время аренды адреса по умолчанию для области – 8 дней, что отличается от значения в Windows NT, где оно составляло 72 часа. Это значение может быть изменено в зависимости от потребностей сети.

- Каждый диапазон IP-адресов может быть представлен только в одной из областей. Если серверы DHCP не будут скоординированы и два сервера будут иметь одинаковые диапазоны адресов в своих областях, тогда один и тот же адрес может быть назначен разным клиентам в одной сети. Также надо быть уверенным, что исключены все статически назначенные IP-адреса из областей.

- Для создания отказоустойчивых областей необходимо настроить 2 (или более) сервера DHCP и разделить диапазоны адресов из каждой области между ними. При такой конфигурации, если один из серверов выйдет из строя, другой будет продолжать распределять допустимые адреса между клиентами.

- Настройки DHCP могут быть осуществлены на 4 различных уровнях: на уровне **Server** (сервера) (установки влияют на все области), **Score** (область) (установки влияют только на область), **Client** (клиент) (установки для зарезервированного клиента) **Class** (класс) (для компьютеров, которые входят в различные, заранее определенные, классы).

Протокол упрощает работу сетевого администратора, который должен вручную конфигурировать только один сервер DHCP. Когда новый компьютер подключается к сети, обслуживаемой сервером DHCP, on запрашивает уникальный IP-адрес, а сервер DHCP назначает его из пула доступных адресов, Этот процесс состоит из четырех шагов:

1. Клиент DHCP запрашивает IP-адрес (DHCP Discover, обнаружение),

2. DHCP-сервер предлагает адрес (DHCP Offer, предложение),

3. Клиент принимает предложение и запрашивает адрес (DHCP Request, запрос) и адрес официально назначается сервером (DHCP Acknowledgement, подтверждение).

Чтобы адрес не "простаивал", сервер DHCP предоставляет его на определенный администратором срок, это называется арендным договором (lease). По истечении половины срока арендного договора клиент DHCP запрашивает его возобновление, и сервер DHCP продлевает арендный договор. Это означает, что когда машина прекращает использовать назначенный IP-адрес (например, в результате перемещения в другой сетевой сегмент), арендный договор истекает, и адрес возвращается в пул для повторного использования.

Протокол DHCP в Microsoft Windows 2000 Server был дополнен новыми функциями, что упростило развертывание, интеграцию и настройку сети.

***Интеграция с DNS.*** Серверы DNS обеспечивают разрешение имен для сетевых ресурсов и тесно связаны со службой DHCP. В Windows 2000 серверы DHCP и клиенты DHCP могут регистрироваться в DNS.

***Улучшенное управление и мониторинг.*** Новая возможность обеспечивает уведомление об уровне использования пула IP-адресов. Оповещение производится при помощи соответствующего значка либо при помощи передачи сообщения.

***Распределение групповых адресов.*** Добавлена возможность назначения групповых адресов. Типичные приложения для групповой работы — конференции или радиотрансляция требуют специальной настройки групповых адресов.

***Защита от появления неправомочных серверов DHCP.*** Наличие нескольких серверов DHCP в одном сегменте сети может привести к конфликту. Новые механизмы позволяют обнаружить конфликт такого рода и деактивизировать работу сервера, обеспечив правильную работу DHCP.

***Защита от подмены серверов.*** Регистрация уполномоченных (авторизированных) серверов DHCP выполняется при помощи Active Directory. Если сервер не обнаружен в каталоге, то он не будет функционировать и отвечать на запросы пользователей.

### 5.2.2. Кластеризация

Кластерные службы, работающие на Windows 2000 Advanced Server и Datacenter поддерживают DHCP-сервер в качестве ресурса кластера, что позволяет повысить доступность DHCP-сервера.

Автоматическая настройка клиентов. Клиенты с поддержкой DHCP. начинающие работу в сети, могут конфигурироваться самостоятельно с использованием временной конфигурации IP (если сервер DHCP недоступен). Клиенты продолжают попытки связаться с сервером DHCP для получения арендного договора в фоновом режиме каждые 5 мин. Автоматическое назначение всегда прозрачно для пользователей. Адреса для такого рода клиентов выбираются из диапазона частных сетевых адресов TCP/IP и не используются в Интернете.

Новые специализированные опции и поддержка пользовательских классов. Сервер DHCP в Windows 2000 может назначать специализированные опции, сокращая время на получение одобрения новой стандартной опции в IETF. Механизм пользовательских классов позволяет применять DHCP в заказных приложениях для сетей масштаба предприятия. Оборудование большинства поставщиков сетевого аппаратного обеспечения также может использовать различные номера опций для различных функций. [3]

# 5.3. Служба DNS

Domain Name System (система доменных имен) – это стандарт службы имен для Интернета, который используется Windows 2000 для помощи клиентам в разрешении имен узлов в их IP-адреса и для поиска служб в сети.

DNS – это распределенная система серверов имен. В этой системе группы серверов имен отвечают за записи, относящиеся к узлам, в доменах и поддоменах. Эти группы называются зонами. Зона является полномочной или ответственной для записей, относящихся к данному домену или группе доменов. Например, Microsoft может иметь несколько серверов, полномочных для домена microsoft.com и все связанные поддомены должны быть частью этого домена. Как следствие, если эти сервера не могут предоставить вам ответ на запрос IP-адреса для имени bluscreen.microsoft.com, то это означает, что его просто не существует.

Серверы имен хранят то, что принято называть записями ресурсов. Записи ресурсов сопоставляют имя узла его IP-адресу или отдельной службы и имени узла. Например, сервер DNS может содержать запись (называемую А записью) для сервера, называемого Cerver2, которому соответствует IP-адрес 147.2.3.45. Если клиент другого сервера DNS запросит связанный IP-адрес, он может быть найден и возвращен (послан) клиенту. Подобным образом, некоторый почтовый сервер может запросить сервер DNS найти почтовый сервер, действующий в домене mailfirma.ru. В данном случае DNS сервер запрашивается на наличие записи о системе обмена почтой (запись МХ), которая предоставляет FGDN (полностью определенное имя домена) почтового сервера, которое, в свою очередь, может быть разрешено в IP-адрес.

Cуществует еще один тип серверов имен, которые не являются полномочными для какой-либо зоны. Эти сервера называются caching-only (только кэширующими) – они просто перенаправляют запросы клиентов другим серверам имен и кэшируют их ответы.

DNS реализована как служба на сервере Windows 2000, а раз так, то она может быть запущена и остановлена, как любая другая служба. Она также может быть добавлена или удалена при помощи программы Add/Remove, вкладка Windows Components. DNS не устанавливается автоматически при установке Windows 2000, поэтому необходимо устанавливать ее вручную. Число серверов DNS, присутствующих в сети зависит от ряда факторов, таких, как потребность в отказоустойчивости, быстродействие и т.д. DNS требуется для установки Active Directory, поскольку домены Active Directory следуют соглашению об именовании DNS. Заметьте, что предыдущий пример рассказывал о DNS разрешении через Internet. Подобным образом DNS может быть использована для разрешения внутренних узлов или для комбинированных ситуаций, имейте это ввиду.

В традиционных конфигурациях DNS имеется как минимум 2 DNS сервера, которые являются полномочными в зоне. Зона – это административная единица DNS, представленная набором серверов DNS, которые ответственны за поддержку информации, относящейся к одному или более домену или поддомену. Один сервер выступает как основной сервер имен и это единственный сервер, который поддерживает перезаписываемую копию файла зоны. Периодически, основной сервер имен реплицирует файл зоны на другой сервер (или сервера), назначенные вторичными серверами имен. Этот сервер (сервера) тоже поддерживает файл зоны, но копию, предназначенную только для чтения. Процесс репликации часто называют передачей зон. Главная причина для того, чтобы иметь 2 или более сервера DNS – это уверенность, что если один из них выйдет из строя, другой может быть доступен для обработки запросов, относящихся к домену, содержащемуся в файле зоны.

Такой тип конфигурации продолжает поддерживаться и в Windows 2000 и на него ссылаются как на «стандартную» конфигурацию DNS. Однако Windows 2000 также поддерживает и другой вид конфигурации, являющийся новинкой в Windows 2000. Эта конфигурация называется «DNS, интегрированная в Active Directory». В данной конфигурации информация о зоне DNS храниться в Active Directory, а не в отдельном наборе файлов. Как следствие, DNS-информация реплицируется автоматически, как часть общей репликации Active Directory, и не требует создания дополнительной топологии репликации. Это не означает, однако, что каждый контроллер домена автоматически становиться сервером DNS. Это означает только, что каждый контроллер домена может стать сервером DNS, если служба DNS будет установлена на компьютер. DNS, интегрированная в Active Directory, также располагает рядом достоинств, таких как, например то, что каждый из серверов DNS может вносить изменения в зону и, в случае отказа одного из серверов, обновления зоны DNS не прекращаются. В стандартной конфигурации DNS обновления невозможны, если прекращает работу основной сервер имен.

Другое большое преимущество Windows 2000 DNS – это то, что она динамическая. Это означает, что узел может регистрировать и отменять регистрацию записей в DNS самостоятельно, включая запись соответствия имени и IP-адреса (А), а также записи служб (это мы обсудим позднее). Преимущество динамической DNS очевидны, так как в предыдущих реализациях DNS все записи требовалось создавать вручную, что отнимало много времени и порождало множество ошибок. Многие сравнивают динамическое обновление DNS с функционированием WINS. Так как эти идеи действительно схожи, помните, что цель WINS – разрешение имен NetBIOS в IP-адрес, в то время как DNS сопоставляет имена узлов их IP-адресам.

DNS используется Windows 2000 не только для разрешения имен узлов в их IP-адреса. Эта служба также помогает системе находить службы в сети, такие как службу аутентификации контроллера домена. Когда пользователь пытается войти в домен, его Windows 2000-система запрашивает DNS о наличии одного или более контроллеров домена на данном физическом сайте. Контроллеры домена автоматически регистрируются в DNS и также регистрируют записи, относящиеся к некоторым, работающим на них, службам. Точно также, клиенты Windows 2000 могут регистрировать себя в DNS самостоятельно, а могут и через сервер DHCP, который дает клиенту его IP-адрес. Оба эти механизма требуют пристального рассмотрения и мы вернемся к ним в нашей серии.

Хотя этот раздел только введение в DNS, хочу привести несколько дополнительных важных заметок о DNS:

- Windows 2000 DNS поддерживает IXFR или инкрементальный (добавочный) трансфер зоны. При этой настройке, если происходят изменения в файле зоны, только эти изменения реплицируются на другие сервера DNS. Если вы помните, в Windows NT DNS поддерживало только АXFR – полный трансфер зоны, при котором изменения в зоне вызывали необходимость репликации всего файла зоны на все дополнительные сервера имен.

- Если используется DNS, интегрированный в Active Directory, то можно активизировать функцию, называемую Secure Dynamic Updates (безопасные динамические обновления). При этом сервер DNS будет позволять обновления или регистрацию записей только с систем, которые имеют правомочные учетные записи в Active Directory. Если эта настройка не активизирована, то любая система может делать изменения в DNS, что представляет, конечно же, угрозу безопасности сети.

### 5.3.1. Планирование внедрения DNS для Active Directory

Прежде чем устанавливать Active Directory в среду Windows 2000, важно разработать реализацию DNS, которая бы соответствовала как вашей системе разрешения имен, так и требованиям Active Directory. DNS необходим Active Directory как для разрешения имен, так и для определения пространства имен, так как доменные имена в Windows 2000 базируются на соглашении об именовании DNS. Как следствие, любой сервер, на который устанавливается Active Directory, должен иметь в своих настройках протокола TCP/IP указание на сервер DNS, который необходимо установить и настроить предварительно. Если не сделаеть это заранее, то инсталляция Active Directory автоматически создаст структуру DNS, которая, возможно, не будет соответствовать вашим пожеланиям.

Первая концепция - это использование DNS для разрешения имен узлов (нахождение соответствующего узлу IP-адреса) или разрешения FQDN (Fully Qualified Domain Name – полностью определенное имя домена) в его IP-адрес. Чтобы напомнить вам, FQDN представляет имя узла в виде доменного имени системы. Например:

www.firma.ru

В этом примере имя узла – левая часть полного имени, а именно www. Имена узла также могут разрешаться при помощи файла HOSTS, который является статическим текстовым файлом и находится в папке %systemroot%\system32\drivers\etc на локальном компьютере. Не стоит путать DNS c WINS, которая ставит в соответствие Netbios имени соответствующий IP-адрес (также имеется текстовый эквивалент данной службы, файл LMHOSTS).

Служба DNS хранит большое число записей ресурсов различного типа, кроме простой записи хоста, т.н. «А» записи. Наиболее используемые типы записей, которые можно встретить в файле зоны, рассмотрены ниже:

**SOA** – представляет из себя запись ресурса начальной записи зоны, и предоставляет информацию о зоне, включая сведения о том, какой сервер является основным, кто отвечает за административный контакт, как часто файл базы данных проверяется на наличие изменений, серийный номер базы данных, значение времени жизни, и т.д.

**A** – представляет уникальный адрес узла в сети, сопоставляя его имя IP-адресу.

**NS** – обозначает доменное имя и связанное с ним FQDN сервера имен, который является полномочным для домена.

**MX** – обозначает, что данный узел является почтовой службой (сервером почты или сервером пересылки) для определенного домена.

**PTR** – предоставляет возможность для обратного просмотра (сопоставляет IP-адресу узла его FQDN). Это позволяет находить имя узла, связанное с IP-адресом. Записи PTR находятся в файле **reverse lookup zone** (зоны обратного просмотра).

**SRV** – сопоставляет отдельные службы одному или нескольким узлам и наоборот. Например, записи могут обозначать сервер как сервер Глобального Каталога, контроллер домена и т.д.

Вторая главная концепция – эта концепция **Зоны**. Зона – это область пространства имен DNS, которая функционирует как административная единица. То есть группа серверов ответственна (имеет полномочие) за записи, относящиеся к некоторому домену или поддомену. Главной причиной для того, чтобы иметь несколько зон, является разделение административной ответственности, так же как и задача пересылки зон.

Существует 5 основных типов серверов DNS. Это основные, вторичные, интегрированные в Active Directory, серверы пересылки и кэширующие сервера.

**Основной сервер DNS** – основным сервером DNS является сервер, который полномочен для зоны. По существу это означает, что в зоне есть только один сервер, на котором можно производить изменения в базе данных зоны.

**Вторичный сервер DNS** – вторичный сервер DNS содержит копии «только для чтения» информации, хранящейся на основном сервере DNS, и получают обновления в ходе передачи зоны. Один вторичный сервер является минимально необходимым, но и другие могут создаваться с целью выравнивания нагрузки и обеспечению отказоустойчивости.

**Интегрированный в Active Directory сервер DNS** – возможен только для серверов DNS на базе OS Windows 2000, в данной реализации DNS файл зоны хранится как объект в Active Directory, а не как несколько файлов на жестком диске. В данном сценарии каждый контроллер домена, на котором установлена DNS по существу действует как основной сервер DNS, допускает изменения в зоне и осуществляет синхронизацию файла зоны через репликацию Каталога. Как следствие, если какой-либо сервер DNS выйдет из строя, любой другой сервер, интегрированный в Active Directory может продолжать осуществлять изменения.

**Кэширующий только** – кэширующий сервер DNS не является полномочным для зоны. Как следствие, он только получает клиентские запросы, осуществляет запросы других серверов DNS, кэширует результаты и посылает ответы клиентам. По умолчанию кэширующий сервер DNS пересылает все запросы, ответы на которые не найдены в его кэше, корневому серверу DNS.

**Сервер пересылки DNS** – серверы DNS могут быть настроены так, что будут пересылать запросы, которые не могут разрешить к какому-либо определенному серверу. Такие серверы называются **forwarder** (сервер пересылки). Серверы пересылки могут впоследствии обрабатывать запросы, вместо других серверов DNS. Это позволяет уменьшить время обработки некоторых запросов по поиску узлов (в Интернете, например), т.к. сервер пересылки обрабатывает запросы и кэширует результат, который потом возвращается к компьютеру, сделавшему запрос. Это может улучшить и скорость и производительность.

### 5.3.2. Новые свойства DNS в Windows 2000

В реализации DNS в Windows 2000 есть ряд изменений по сравнению с NT 4. Наиболее важные из них это – поддержка записей служб, динамическая DNS, безопасное динамическое обновление, добавочная передача зоны и интегрирование с Active Directory.

**Записи для служб** – в реализации DNS в Windows 2000 поддерживаются записи для такого важного типа ресурсов, как записи служб (часто упоминаемые как SRV записи). Записи служб позволяют клиентам запрашивать DNS-поиск для систем, на которых запущены определенные службы, такие как Глобальный Каталог (который обозначается как GC-запись).

**Динамическая DNS** – в традиционных реализациях DNS все записи было необходимо создавать и изменять вручную на DNS сервере, что могло отнимать огромное количество времени. Реализация DNS в Windows 2000 поддерживает RFC 2136 и обычно называется Dynamic DNS или DDNS. В данной реализации клиенты имеют возможность автоматически обновлять свои записи, которые главным образом используются в среде, где клиенты подключаются к серверу DHCP для получения IP-адресов. Windows 2000 является единственной OS фирмы Microsoft (теперь еще и Windows XP), которая поддерживает динамическое обновление. Однако можно настроить сервер DHCP в Windows 2000 так, что он сможет обновлять DNS на стороне клиентов, что позволяет клиентам, работающим под другими (не-Windows 2000) OS, обновлять информацию о себе в DNS. Динамическая DNS также очень удобна для контроллеров домена, которые также могут автоматически регистрировать записи своих сервисов, в противном случае, все это было бы необходимо делать вручную.

**Безопасное динамическое обновление** – если DNS зона является интегрированной в Active Directory, то Windows 2000 позволяет вам использовать нечто, что называется безопасным динамическим обновлением. Заметьте, что простые динамические обновления могут быть потенциально опасными, потому что любой клиент может быть зарегистрирован в DNS, так как динамическая DNS только отвечает на запросы, но не аутентифицирует их. Если установлено безопасное динамическое обновление, только пользователь или система, которые имеют соответствующие разрешения на связанных ACL (access control list – списках контроля доступа) для зоны, могут добавлять записи в DNS. По умолчанию Группа Аутентифицированных Пользователей имеет необходимые разрешения. Клиентские системы сначала предпринимают попытку использовать обычный запрос по умолчанию и, если он будет отвергнут, безопасное обновление.

Добавочная передача зоны – реализация NT 4 DNS поддерживает только **AXFR**, или полную передачу зоны. При этой конфигурации каждый раз, когда основной сервер имен осуществлял передачу зоны вторичному серверу, файл базы данных зоны передавался целиком, даже если в нем произошло единичное изменение. Windows 2000 поддерживает **IXFR** или добавочную передачу зоны. В данной реализации, только изменения передаются в ходе передачи зоны, вместо передачи всего файла базы данных зоны.

**Интеграция с Active Directory** – Windows 2000 продолжает поддерживать традиционную реализацию по схеме основной/вторичный сервера DNS. В данном сценарии, изменения в файле зоны могут быть сделаны только на основном сервере, так как только он содержит редактируемую копию файла зоны. В Windows 2000 вводится новая концепция – DNS, интегрированная в Active Directory. В этой реализации файл зоны DNS и связанная с ним информация хранится как объект в Active Directory вместо того, чтобы находиться в папке DNS на жестком диске. Эта интеграция позволяет любому контроллеру домена, на котором запущена служба DNS, делать изменения в базе данных DNS, при этом изменения в зоне реплицируются как часть процесса репликации Active Directory. Это также позволяет сделать службу DNS более отказоустойчивой. В традиционной среде DNS, если основной сервер имен выходит из строя, все динамические изменения в DNS становятся невозможными, так как редактируемая копия зоны недоступна. В DNS, интегрированной в Active Directory, все DNS сервера могут осуществлять обновления. Традиционные сервера DNS могут продолжать существовать в такой среде – они могут быть вторичными и использовать сервер DNS, интегрированный в Active Directory, как основной сервер для получения файла зоны.

### 5.3.3 Настройка сервера DNS.

Настройка и изменение конфигурации сервера DNS могут понадобиться по разным причинам, например:

1. При изменении имени компьютера-сервера

2. При изменении имени домена для компьютера-сервера

3. При изменении IP-адреса компьютера-сервера

4. При удалении сервера DNS из сети

5. При изменении основного сервера (primary server) зоны

***Управление клиентами***

Для клиентов Windows конфигурация DNS при настройке свойств TCP/IP для каждого компьютера включает следующие задачи:

1. Установка имени хоста DNS для каждого компьютера или сетевого подключения.

2. Установка имени родительского домена, которое помещается после имени хоста, чтобы формировать полное (fully qualified) имя домена для каждого клиента.

3. Установка основного DNS-сервера и списка дополнительных DNS-cep-веров, которые будут использоваться, если основной сервер недоступен.

4. Установка очередности списка поиска доменов, используемого в запросах для дополнения не полностью заданного имени компьютера.

***Управление зонами***

После добавления зоны при помощи оснастки DNS можно управлять следующими общими свойствами зоны:

1. Запрещать или разрешать использование зоны

2. Изменять или преобразовывать тип зоны

3. Разрешать или запрещать динамическое обновление зоны

Также можно настраивать начальные записи зоны (Start Of Authority, SOA), ресурсные записи, делегирование зон, списки оповещения, использование просмотра WINS, а также управлять зонами обратного просмотра (reverse zone), необходимыми для обратного разрешения имен — из адреса в имя.

***Мониторинг и оптимизация***

В Windows 2000 Advanced Server можно производить мониторинг и по его результатам оптимизировать настройки службы DNS при помощи:

1. Системного монитора (Performance Monitor)

2. Опций протоколирования

3. Статистики по DNS-серверу

4. Настройки дополнительных параметров

## 5.4. Служба WINS

Служба WINS (Windows Internet Name Service, служба имен Windows) обеспечивает поддержку распределенной базы данных для динамической регистрации и разрешения имен NetBIOS для компьютеров и групп, используемых в сети. Служба WINS отображает пространство имен NetBIOS и адресное пространство IP друг на друга и предназначена для разрешения имен NetBIOS в маршрутизируемых сетях, использующих NetBIOS поверх TCP/IP. Имена NetBIOS используются более ранними версиями операционных систем Microsoft для идентификации компьютеров и других общедоступных ресурсов. [12]

Хотя протокол NetBIOS может применяться с другими сетевыми протоколами, помимо TCP/IP (например, NetBEUI или IPX/SPX), служба WINS была разработана для поддержки NetBIOS поверх TCP/IP (NetBT). WINS упрощает управление пространством имен NetBIOS в сетях на базе TCP/IP. WINS применяется для распознавания имен NetBIOS, но для ускорения разрешения имен клиенты должны динамически добавлять, удалять или модифицировать свои имена в WINS.

### 5.4.1. Новые возможности WINS в Windows 2000

В Windows 2000 WINS обеспечивает следующие расширенные возможности:

1. Постоянные соединения. Теперь можно настроить каждый WINS-сервер на обслуживание постоянного соединения с одним или большим количеством партнеров репликации. Это увеличивает скорость репликации и снижает затраты на открытие и завершение соединений.

2. Управление "захоронением". Можно вручную отмечать записи для захоронения (отметка для дальнейшего удаления, tombstoning). Состояние "захоронения" записи копируется для всех серверов WINS, что предотвращает восстановление копии из баз данных других серверов.

3. Улучшенная утилита управления. Утилита управления WINS реализована в виде оснастки ММС, что упрощает использование WINS для администратора.

4. Расширенная фильтрация и поиск записей. Улучшенная фильтрация и новые поисковые функции помогают находить записи, показывая только записи, соответствующие заданным критериям. Эти функции особенно полезны для анализа очень больших баз данных WINS.

5. Динамическое стирание записей и множественный выбор. Эти особенности упрощают управление базой данных WINS. При помощи оснастки WINS можно легко манипулировать с одной (или более) записью WINS динамического или статического типа.

6. Проверка записей и проверка правильности номера версии. Эти возможности проверяют последовательность имен, сохраненных и скопированных на серверах WINS. Проверка записей сравнивает IP-адреса, возвращаемые по запросу по имени NetBIOS с различных серверов WINS. Проверка правильности номера версии проверяет номер владельца таблицы отображения "адрес-версия".

7. Функция экспорта. При экспорте данные WINS сохраняются в текстовом файле с запятыми в качестве разделителей. Можно импортировать этот файл в Microsoft Excel и другие программы для анализа и составления отчетов.

8. Увеличенная отказоустойчивость клиентов. Клиенты под управлением Windows 2000 или Windows 98 могут использовать более двух серверов WINS (максимально — 12 адресов) на интерфейс. Дополнительные адреса серверов WINS будут использоваться, если первичные и вторичные серверы WINS не отвечают на запросы.

9. Консольный доступ только для чтения к WINS Manager. Эта возможность предоставляется группе Пользователи WINS (WINS Users), которая автоматически создается при установке сервера WINS. Добавляя членов к этой группе, можно предоставить доступ только для чтения к информации о WINS. Это позволяет пользователю-члену группы просматривать, но не изменять информацию и свойства, хранящиеся на определенном сервере WINS.[1]

### 5.4.2. Компоненты службы WINS

Основные компоненты WINS — сервер WINS и клиенты WINS, а также посредники WINS (WINS proxy).

***Серверы WINS.*** Сервер WINS обрабатывает запросы на регистрацию имен от клиентов WINS, регистрирует их имена и IP-адреса и отвечает на запросы разрешения имен NetBIOS от клиентов, возвращая IP-адрес по имени, если это имя находится в базе данных сервера (рис. 17.8). Сервер WINS поддерживает базу данных WINS.

***Клиенты WINS.*** Клиенты WINS регистрируют свои имена на сервере WINS, когда они запускаются или подключаются к сети.

Microsoft поддерживает клиентов WINS на платформах Windows 2000 Server/Professional, Windows NT Server/Workstation, Windows 9x, Windows for Workgroups, Microsoft LAN Manager, MS-DOS, OS/2, Linux/Unix (с установленной службой Samba) [7].

Клиенты WINS обращаются к серверу WINS, чтобы зарегистрировать/об-новить/удалить имя клиента в базе данных WINS, а также для разрешения имен пользователей, имен NetBIOS, имен DNS и адресов IP.

***Посредники WINS.*** Посредник WINS — клиентский компьютер WINS, настроенный так, чтобы действовать от имени других хостов, которые не могут непосредственно использовать WINS .

### 5.4.3. Планирование сети с использованием WINS

Перед установкой серверов WINS в сети необходимо решить следующие задачи:

Определить число необходимых серверов WINS

Спланировать партнеров репликации

Оценить влияние трафика WINS на самых медленных соединениях

Оценить уровень отказоустойчивости в пределах сети для WINS

Составить и оценить план инсталляции WINS

До настройки репликации нужно тщательно спроектировать топологию репликации WINS. В глобальных сетях это очень важно для успешного развертывания и использования WINS.

Настройка статического отображения:

Запись, отображающая имя в IP-адрес, может быть добавлена в базу данных WINS двумя способами:

1. Динамически (клиентами WINS, непосредственно при связи с сервером WINS).

2. Статически (вручную, администратором, при помощи оснастки WINS или утилит командной строки).

Статические (добавляемые администратором вручную) записи полезны, когда нужно добавить отображение "имя-адрес" к базе данных сервера для компьютера, который непосредственно не использует WINS. Например, в некоторых сетях серверы под управлением других операционных систем не могут регистрировать имя NetBIOS непосредственно на сервере WINS. Хотя эти имена можно было бы добавить с помощью файла Lmhosts или через запрос

### 5.4.4. Управление базой данных WINS

Оснастка WINS обеспечивает поддержку, просмотр, копирование и восстановление базы данных WINS. Основные задачи по работе с базой:

Сжатие базы

Резервное копирование базы

Проверка целостности базы

Переход от WINS к DNS

В сетях, использующих только Windows 2000, можно уменьшить или даже устранить применение WINS. Удаление установленных серверов WINS из сети называется отзывом (decommissioning).

После развертывания сервера DNS в сети отзыв сервера WINS выполняется в такой последовательности:

1. Клиентские компьютеры перенастраиваются, чтобы они не использовали WINS, а только DNS.

2. На каждом сервере WINS по отдельности запускается процесс отзыва:

• В дереве WINS выбрать сервер WINS, который нужно отозвать, затем выбрать опцию Активные регистрации (Active Registrations).

• В меню Действие (Action) выберать пункт «Найти по владельцу» (Show records for the sleeted owner).

• В появившемся окне в списке только для выбранного владельца (only for selected owner) выбрать сервер WINS, который необходимо отозвать, и нажать кнопку ОК.

• В подокне подробного просмотра выделить все элементы.

• В меню Действие (Action) выберать команду Удалить (Delete).

• В диалоговом окне Подтверждение удаления записей (Confirm WINS Record Delete) установить переключатель Реплицировать удаление записи на другие серверы (Tombstone WINS records on all WINS servers) переключателя и нажмать кнопку ОК.

• Подтвердить удаление, нажав кнопку Да (Yes) в окне запроса.

•В дереве выберать элемент Партнеры репликации (Replication Partners).

• В меню Действие (Action) выбрать команду Запустить репликацию

(Replicate Now).

• После проверки репликации выбранных записей на другие серверы остановить и удалить службу WINS на отозванном сервере.

3. Делается необязательная настройка для уменьшения и переадресации трафика WINS. Может потребоваться настроить дополнительное разрешение имен DNS через WINS.

После заключительного шага процесса отзыва WINS можно настроить клиентские компьютеры под управлением Windows 2000, чтобы они не использовали поддержку NetBIOS поверх TCP/IP (NetBIOS over TCP/IP). Этот шаг нужен, только если надо уменьшить трафик запросов имени NetBIOS и трафик регистрации WINS. Однако в большинстве сетей ограниченное применение WINS какое-то время еще будет необходимо.

## 5.5. Конфигурирование сервера

Сетевая операционная система выполняется на сетевом сервере. С другой стороны, компьютеры-клиенты могут работать под управлением различных операционных систем. Чтобы операционная система клиента могла использовать сеть, нужно установить специальные драйверы, которые позволят плате сетевого интерфейса компьютера-клиента связаться с сетью. Эти драйверы работают подобно драйверам принтера, позволяющим прикладным программам посылать информацию на принтер. Программное обеспечение сетевого драйвера дает возможность программам посылать и принимать информацию по сети. Каждый компьютер в сети содержит одну или более плат сетевого интерфейса, которые соединяют компьютер с сетью.

### 5.5.1. Выбор сервера

Очевидно, что производительность ЛВС не в последнюю очередь зависит от компьютера, используемого в качестве сервера. При использовании Windows 2000 Server необходимо ориентироваться на наиболее высокоскоростной компьютер. В этом случае, как всегда, существует возможность выбора между готовыми серверами, предлагаемыми производителями и поставщиками компьютерной техники, и серверами самостоятельной сборки. При наличии определенного опыта, самостоятельно собранный под заказ сервер может составить альтернативу готовому продукту. Большое разнообразие компонентов не дает возможности назвать конкретные виды «железа» для закупки и сборки. Поэтому следует обратить внимание на следующие моменты. [13]

1. На вопрос об используемой шине ответ однозначен – PCI. Помимо высокой производительности (за счет 64-битной разрядности шины), PCI – компоненты допускают программное конфигурирование. Благодаря последнему обстоятельству, возможные конфликты между подключаемыми аппаратными ресурсами почти всегда предотвращаются автоматически.
2. Windows 2000 Server изначально предъявляет высокие требования к объему оперативной памяти. И они еще более возрастают в случае применения сетевого сервера (здесь объем ОЗУ должен быть не менее 64 Мб).
3. В сервере должны использоваться, как минимум, винчестеры и соответствующие адаптеры SCSI. Новейшие диски данного стандарта при частоте вращения шпинделя 15000 об/мин обеспечивают максимально высокую скорость передачи данных практически независящую от загрузки дисковой подсистемы.
4. Идеальным корпусом будет специальный корпус для сервера, снабженные мощными блоками питания, дополнительными вентиляторами, съемными заглушками и защитной передней панелью. В качестве более экономичного решения допустимо использование корпусов типа Big Tower, прошедших сертификацию фирмы-производителя материнской платы.
5. Скоростной привод CD-ROM не только сэкономит время при установке ОС и прикладного ПО, но и окажется чрезвычайно полезным при работе с централизованной справочной системой.
6. Так как все подключенные к сети рабочие станции будут постоянно обращаться к серверу, одним из его важнейших компонентов является производительная 32-ух или 64-х битная сетевая карта. Она должна эффективно управлять информационным обменом, то есть иметь сопроцессор, принимающий на себя основные функции центрального процессора по обработке поступающих на сервер данных. Для обеспечения дополнительной надежности можно использовать 2 и более сетевых карты одновременно.

Исходя из вышеизложенного, предлагается следующая модель корпоративного сервера Klondike President 2000A.

Klondike President 2000A - универсальный сервер среднего уровня. Может использоваться в качестве сервера служб обмена электронными сообщениями, сервера службы доменных имен, сервера службы доступа к информационным ресурсам. Построен на базе производительной материнской платы Intel SDS2.

Таблица 5.1.

Конфигурация сервера.

|  |  |
| --- | --- |
| **Состав системного блока** | |
| Процессор | 2 Intel Xeon DP 1,8 - 2,8 ГГц |
| Кэш-память | 512 Кбайт (L2) |
| Чипсет | ServerWorks Server Set GC-LE |
| Оперативная память | до 12 Гбайт ECC DDR200/266 |
| Слоты расширения | 3 x PCI 32-бит/33 МГц  2 x PCI 64-бит/100 МГц  1 x PCI 64-бит/133 МГц |
| Контроллеры жестких дисков | - Adaptec AIC-7899W Ultra3Wide SCSI (2 канала, встроенный) |
| Жесткие диски | 18 – 146 Гбайт (Ultra160 SCSI, 10000-15000 об/мин) |
| Места для жестких дисков | 10 x 3,5" (горячая замена) |
| Устройства ввода/вывода | FDD 3,5" 1,44 Мбайт  CD-ROM 50x |
| Места для дополнительных устройств | 1 x 3.5" (занято FDD)  3 x 5,25 (одно занято CD-ROM) |
| Устройство резервного копирования | - 4 мм SCSI ленточные накопители DAT стандарта DDS-3 и DDS-4 емкостью до 40 Гбайт |
| Видеоконтроллер | PCI, ATI Rage XL 8 Мбайт (встроенный) |
| Сетевой адаптер | Intel PRO/100+  Intel PRO/1000 XT |
| Порты ввода/вывода | COM1, COM2, LPT, 4 USB |
| Корпус | Hudson3 - Tower (HxWxD - 45x22x69 cм) |
| Блоки питания | - 2\*350 Вт |
| Диагностика неисправностей | отказ вентиляторов охлаждения (предсказание отказа), отказ жестких дисков (предсказание отказа, SMART), отказ питающих напряжений, отказ блоков питания, ошибки в памяти (с указанием сбойного модуля памяти физического адреса), ошибки PCI, сбой или превышение рабочей температуры процессоров, превышение рабочей температуры электронных компонентов, превышение рабочей температуры в отсеках для жестких дисков, зависание операционной системы |
| Устранение неисправностей | автоматическая коррекция ошибок в памяти, автоматическое отключение неисправного процессора (FRB level 1,2,3), автоматическая перезагрузка или выключение системы в критических ситуациях, автоматическая аппаратная перезагрузка при зависании операционной системы. |
| Безопасность | контроль трех датчиков открытия корпуса и отсека с жесткими дисками, блокирование клавиатуры и мыши, блокирование кнопок выключения питания и перезагрузки, выключение видео и дисковода, доступ по паролю. |
| ПО управления | Intel Server Management |
| Предустанавливаемая ОС | Microsoft, |

### 5.5.2. Установка Windows 2000 Advanced Server

Компьютер, на который Вы хотите установить операционную систему, не должен содержать форматированных разделов. Раздел на жестком диске для установки Windows 2000 Advanced Server в качестве изолированного сервера рабочей группы можно создать непосредственно в процессе установки.

На Вашем компьютере должна работать MS-DOS или любая версия Windows. Кроме того, он должен уметь обращаться к каталогу Bootdisk установочного компакт-диска с Windows 2000 Advanced Server. Если Ваш компьютер настроен для загрузки с CD-ROM, Вы можете установить Windows 2000, не используя установочные дискеты.

#### *5.5.2.1. Запуск процедуры предварительного копирования файлов и текстового режима Windows 2000 Advanced Server*

Вставьте загрузочный диск Windows 2000 Advanced Server и перезагрузите компьютер

1. После перезапуска компьютера появится сообщение, что выполняется проверка вашей системной конфигурации, и вскоре откроется окно Windows 2000 Setup.

Обратите внимание на серую строку внизу экрана. В ней сообщается, что выполняется проверка компьютера и загрузка Windows 2000 Executive — минимальной версии ядра Windows 2000.

2. Установщик произведет загрузку HAL, шрифтов, драйверов шины и других программ, обеспечивающих работу материнской платы, шины и других аппаратных средств вашего компьютера. Кроме того, будут загружены исполнимые файлы Windows 2000 Setup.

3. Установщик произведет загрузку драйверов контроллера дисковода и инициализацию драйверов, обеспечивающих поддержку доступа к дисководу. Во время этого процесса Setup может несколько раз останавливаться.

4. Установщик загрузит драйверы периферийных устройств, например драйвер дисковода и файловых систем, после чего будет выполнена инициализация исполняемой части Windows 2000 и загрузка оставшихся установочных файлов.

Если Вы устанавливаете пробную версию Windows 2000, программа установки предупредит Вас об этом.

1. Прочитав сообщение установщика Windows 2000, нажмите Enter. Заметьте, что программа установки позволяет Вам произвести не только первоначальную установку, но и восстановить поврежденную версию Windows 2000.
2. Прочитайте сообщение, содержащееся в окне **Welcome To Setup,** и нажмите Enter для продолжения установки. Откроется окно **License Agreement.**
3. Прочитайте лицензионное соглашение. Для прокрутки текста пользуйтесь клавишей Page Down.
4. Выберите I Accept The Agreement, нажав клавишу F8.

Откроется окно Windows 2000 Advanced Server Setup, где Вам предлагается выбрать область диска (или уже существующий раздел) для установки Windows 2000. На этом этапе Вы можете создавать и удалять разделы на жестком диске.

Если жесткий диск ранее не содержал разделов, то Вы увидите на диске неразмеченное пространство.

9. Убедившись, что выбрано Unpartitioned space (неразмеченное пространство), нажмите клавишу C. Появится сообщение о создании нового раздела с указанием минимально и максимально возможных размеров этого раздела.

10. Выбрав размер раздела (минимум 2 Гб), нажмите Enter. Новый раздел будет назван С: New (Unformatted).

1. Убедившись, что выбран новый раздел, нажмите Enter. Установщик предложит выбрать файловую систему для нового раздела.
2. Воспользовавшись клавишами управления курсором, выберите Format The Partition Using The NTFS File System и нажмите Enter. Установщик отформатирует раздел под NTFS, проверит жесткий диск на наличие ошибок, способных повлечь сбои в установке, после чего скопирует файлы на диск. Это займет несколько минут.

По завершении копирования компьютер будет перезагружен.

13. Выньте установочный диск.

14. Программа установки скопирует дополнительные файлы, затем перезагрузит ваш компьютер и запустит мастер установки Windows 2000.

#### *5.5.2.2. Графический режим установки и сбор информации*

С этого момента установщик начинает работать в графическом режиме.

1. В окне мастера установки Windows 2000 щелкните кнопку Next для сбора информации о компьютере.

Установщик сконфигурирует папки и разрешения NTFS для файлов операционной системы. После этого выполняется поиск устройств, подключенных к компьютеру, а также установка и конфигурирование драйверов этих устройств. Это займет несколько минут.

2. Убедившись, что в системных и пользовательских параметрах, а также для раскладки клавиатуры указаны нужные Вам язык и регион, щелкните Next.

3. На странице **Personalize Your Software** введите Ваше имя в поле Name (Имя) и имя Вашей организации в поле **Organization** (Организация), затем щелкните Next.

Эти данные используются в дальнейшем для генерации имени компьютера по умолчанию, а также приложениями — для регистрации ПО и идентификации документов.

Откроется окно **Licensing Modes** с предложением выбрать режим лицензирования. По умолчанию устанавливается режим лицензирования **Per Server** (на сервер). Установщик попросит Вас ввести количество приобретенных для этого сервера лицензий.

4. Щелкните переключатель **Per Server Number Of Concurrent Connections** и установите число одновременных соединений равным приобретённому количеству лицензий (для этого введите количество лицензий в соответствующее поле). Далее щелкните Next.

В поля **Administrator Password и Confirm Password** введите строчными буквами пароль администратора и щелкните кнопку Next. Пароль чувствителен к регистру.

В реальных ситуациях для пароля администратора рекомендуется выбирать более сложное сочетание символов (которое было бы трудно угадать). В частности, Microsoft рекомендует, чтобы пароль содержал прописные и строчные буквы, а также числа и другие символы (например, Lp6\*g9).

Откроется окно **Windows 2000 Components,** в котором перечислены доступные компоненты Windows 2000. Щелкните Next.

После установки Windows 2000 дополнительные компоненты устанавливаются средствами **Add/Remove Programs** панели управления. Пока же Вам нужно установить только компоненты, выбранные по умолчанию. Дополнительные компоненты Вы установите позже.

Если во время установки на Вашем компьютере был обнаружен модем, откроется окно **Modem Dialing Information.** В открывшееся окно **Modem Dialing Information** введите в него код региона или города и щелкните Next. Откроется окно **Date And Time Settings.**

После перезагрузки будет запущена только что установленная версия Windows 2000 Advanced Server.

#### *5.5.2.3. Завершение установки оборудования*

На этом этапе выполняется поиск устройств Plug and Play, не обнаруженных ранее.

1. Войдите в систему, нажав Ctrl+Alt+Delete.
2. В диалоговом окне **Enter Password** введите **administrator** в поле **User Name и пароль** — в поле **Password.**
3. Щелкните кнопку **ОК.**
4. Если Windows 2000 найдет устройства, которые не были обнаружены при установке, откроется окно мастера **Found New Hardware** с сообщением, что Windows 2000 устанавливает соответствующие драйверы.

Если откроется окно мастера **Found New Hardware,** убедитесь, что флажок **Restart The Computer When I Click Finish** не установлен, и щелкните кнопку **Finish** для завершения работы мастера Found New Hardware.

Откроется окно **Configure Your Server,** позволяющее Вам сконфигурировать множество различных параметров и служб.

1. Установите флажок **I Will Configure This Server Later** и щелкните кнопку Next.
2. В следующем окне сбросьте флажок **Show This Screen At Startup.**
3. Закройте окно **Configure Your Server.**

Установка Windows 2000 Advanced Server завершена, и Вы вошли в систему под учетной записью Administrator. [11]

### 5.5.3. Управление в среде Windows 2000 Advanced Server

После успешной установки Windows 2000 Server выполняется настройка пользователей.

Основным элементом централизованного администрирования в Windows 2000 Server является домен. Домен - это группа серверов, работающих под управлением Windows 2000 Server, которая функционирует, как одна система. Все серверы Windows 2000 в домене используют один и тот же набор учетных карточек пользователя, поэтому достаточно заполнить учетную карточку пользователя только на одном сервере домена, чтобы она распознавалась всеми серверами этого домена.

Связи доверия - это связи между доменами, которые допускают сквозную идентификацию, при которой пользователь, имеющий единственную учетную карточку в домене, получает доступ к целой сети. Если домены и связи доверия хорошо спланированы, то все компьютеры Windows 2000 распознают каждую учетную карточку пользователя и пользователю надо будет ввести пароль для входа в систему только один раз, чтобы потом иметь доступ к любому серверу сети. [3]

Группирование компьютеров в домены дает два важных преимущества сетевым администраторам и пользователям. Наиболее важное - серверы домена составляют (формируют) единый административный блок, совместно использующий службу безопасности и информацию учетных карточек пользователя. Каждый домен имеет одну базу данных, содержащую учетные карточки пользователя и групп, а также установочные параметры политики безопасности. Все серверы домена функционируют либо как первичный контроллер домена, либо как резервный контроллер домена, содержащий копию этой базы данных. Это означает, что администраторам нужно управлять только одной учетной карточкой для каждого пользователя, и каждый пользователь должен использовать (и помнить) пароль только одной учетной карточки. Расширяя административный блок с единственного компьютера на целый домен, Windows 2000 Server сохраняет усилия администраторов и время пользователей.

Второе преимущество доменов сделано для удобства пользователей: когда пользователи просматривают сеть в поисках доступных ресурсов, они видят сеть, сгруппированную в домены, а не разбросанные по всей сети серверы и принтеры.

### 5.5.4. Требования к домену

Минимальное требование для домена - один сервер, работающий под управлением Windows 2000 Server, который служит в качестве первичного контроллера домена и хранит оригинал базы данных учетных карточек пользователя и групп домена. В дополнение к сказанному, домен может также иметь другие серверы, работающие под управлением Windows 2000 Server и служащие в качестве резервных контроллеров домена, а также компьютеры, служащие в качестве стандартных серверов, серверов LAN Manager 2.x, клиентов Windows 2000 Workstation и других клиентов, как например, работающих с MS-DOS.

Первичный контроллер домена должен быть сервером, работающим под управлением Windows 2000 Server. Все изменения базы данных, учетных карточек пользователя и групп домена должны выполняться в базе данных первичного контроллера домена.

Резервные контроллеры домена, работающие под управлением Windows 2000 Server, хранят копию базы данных учетных карточек домена. База данных учетных карточек копируется во все резервные контроллеры домена.

Все резервные контроллеры домена дополняют первичный контроллер и могут обрабатывать запросы на начала сеанса от пользователей учетных карточек домена. Если домен получает запрос на начало сеанса, первичный контроллер домена или любой из резервных контроллеров домена может идентифицировать попытку начала сеанса.

Дополнительно к первичным и резервным контроллерам домена, работающим под управлением Windows 2000 Server, есть другой тип серверов. Во время установки Windows 2000 они определяются, как “серверы”, а не контроллеры домена. Сервер, который входит в домен, не получает копию базы данных пользователей домена. [12]

### 5.5.5. Выбор модели организации сети

Проанализировав организационно-штатную структуру предприятия, можно заключить, что оптимальным выбором является модель основного домена. Ее достоинства и недостатки сведены в табл. 5.1.

Таблица 5.2

Преимущества и недостатки модели основного домена.

|  |  |
| --- | --- |
| Преимущества | Недостатки |
| Учетные карточки пользователей могут управляться централизовано. | Ухудшение производительности в случае, если домен будет дополнен большим числом пользователей и групп. |
| Ресурсы сгруппированы логически. Что актуально в связи с территориальной разбросанностью рабочих станций предприятия. | Локальные группы должны быть определены в каждом домене, где они будут использоваться. |
| Домены отделений могут иметь своих собственных администраторов, которые управляют ресурсами в отделе. Что является актуальным для предприятия так как в компьютерных классах обязательно должно быть администрирование сети. |  |
| Глобальные группы должны быть определены только один раз (в основном домене). |  |

## 5.6. Служба Routing and Remote Access

Служба Routing and Remote Access (Маршрутизация и удаленный до­ступ) — это фактически полноценный многофункциональный марш­рутизатор, поддерживающий множество протоколов. Используйтся Routing and Remote Access для поддержки маршру­тизации в частных сетях и между разными сегментами сети.

Функции, обеспечиваемые службой Routing and Remote Access:

поддержка множества протоколов, в том числе IP, IPX и AppleTalk;

* *одноадресная* (unicast) IP-маршрутизация средствами протоколов:
  1. Open Shortest Path First (OSPF);
  2. Routing Information Protocol (RIP) версий 1 и 2, протокол маршрутизации IP;
* *многоадресная* (multicast) IP-маршрутизация средствами маршрутизатора IGMP (Internet Group Membership Protocol), в том числе при работе в режиме прокси-сервера;
* маршрутизация вызова по требованию по коммутируемым WAN-подключениям;
* поддержка VPN-сетей по туннельному протоколу Point-to-Point Tunneling Protocol (PPTP);
* поддержка VPN-сетей по туннельному протоколу Layer Two Tunneling Protocol (L2TP);
* фильтрация IP- и IPX-пакетов;
* агент ретрансляции DHCP (DHCP Relay Agent) для IP;
* поддержка носителей, в том числе Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), ATM (Asynchronous Transfer Mode), Integrated Services Digital Network (ISDN), T-Carrier, Frame Relay, xDSL, кабельных модемов, Х.25 и аналоговых модемов.

## 5.7. Измерение сетевого трафика

Наблюдение за сетевой активностью включает:

* наблюдение за производительностью сервера;
* измерение общего сетевого трафика.

С сетевой активностью связано большое количество счетчиков. Все сетевые компоненты - Server, Redirector, протоколы NetBIOS, NWLink, TCP/IP - генерируют набор статистических параметров. Ненормальное значение сетевого счетчика часто говорит о проблемах с памятью, процессором или диском сервера. Следовательно, наилучший способ наблюдения за сервером состоит в наблюдении за сетевыми счетчиками в сочетании с наблюдением за такими счетчиками, как %Processor Time, %Disk Time и Pages/sec.

Например, если сервер показывает резкое увеличение счетчика Pages/sec одновременно с падением счетчика Total bytes/sec, то это может говорить о том, что компьютеру не хватает физической памяти для сетевых операций.

Расчет сетевой нагрузки



где : n – количество запросов;

 - продолжительность передачи ед.объема информации

Т – время работы сети

А=0.25

Во время работы пользователя в среднем за один диалоговый шаг передается 1,5 - 2,0 Кб данных, а одна операция требует в среднем прохода по 3 - 4 экранам, поэтому средний объем операции принимается равным 16000 байт. Для того, чтобы обеспечить требуемое время ответа (response time) утилизация сети не должна превышать 50%. Оптимальной считает нагрузка 30% , в нашей сети получена нагрузка 25%, что свидетельствует об оптимальной работе сети.

# 6. Защита информации в сети

Исследование и анализ многочисленных случаев воздействий на информацию и несанкционированного доступа к ней показывают, что их можно разделить на случайные и преднамеренные.

Для создания средств защиты информации необходимо определить природу угроз, формы и пути их возможного проявления и осуществления в автоматизированной системе. Для решения поставленной задачи все многообразие угроз и путей их воздействия приводится к простейшим видам и формам, которые были бы адекватны их множеству в автоматизированной системе.

Исследование опыта проектирования, изготовления, испытаний и эксплуатации автоматизированных систем говорят о том, что информация в процессе ввода, хранения, обработки и передачи подвергается различным случайным воздействиям.

Причинами таких воздействий могут быть:

- отказы и сбои аппаратуры;

- помехи на линии связи от воздействий внешней среды;

- ошибки человека как звена системы;

- системные и системотехнические ошибки разработчиков;

- структурные, алгоритмические и программные ошибки;

- аварийные ситуации;

- другие воздействия.

Преднамеренные угрозы связаны с действиями человека, причинами которых могут быть определенное недовольство своей жизненной ситуацией, сугубо материальный интерес или простое развлечение с самоутверждением своих способностей, как у хакеров, и т.д.[12]

Нет никаких сомнений, что на предприятии произойдут случайные или преднамеренные попытки взлома сети извне. В связи с этим обстоятельством требуется тщательно предусмотреть защитные мероприятия.

Для вычислительных систем характерны следующие штатные каналы доступа к информации:

* терминалы пользователей, самые доступные из которых это рабочие станции в компьютерных классах;
* терминал администратора системы;
* терминал оператора функционального контроля;
* средства отображения информации;
* средства загрузки программного обеспечения;
* средства документирования информации;
* носители информации;
* внешние каналы связи.

Принято различать пять основных средств защиты информации:

* технические;

- программные;

- криптографические;

* организационные;

- законодательные.

## 6.1. Анализ возможностей системы разграничения доступа Windows 2000 Advanced Server

Windows 2000 Advanced Server имеет средства обеспечения безопасности, встроенные в операционную систему. Ниже рассмотрены наиболее значимые из них.

#### *6.1.1. Слежение за деятельностью сети*

Windows 2000 Server дает много инструментальных средств для слежения за сетевой деятельностью и использованием сети. ОС позволяет просмотреть сервер и увидеть, какие ресурсы он использует; увидеть пользователей, подключенных к настоящему времени к серверу и увидеть, какие файлы у них открыты; проверить данные в журнале безопасности; записи в журнале событий; и указать, о каких ошибках администратор должен быть предупрежден, если они произойдут. [3]

#### *6.1.2. Начало сеанса на рабочей станции*

Всякий раз, когда пользователь начинает сеанс на рабочей станции Windows 98, экран начала сеанса запрашивает имя пользователя, пароль и домен. Затем рабочая станция посылает имя пользователя и пароль в домен для идентификации. Сервер в домене проверяет имя пользователя и пароль в базе данных учетных карточек пользователей домена. Если имя пользователя и пароль идентичны данным в учетной карточке, сервер уведомляет рабочую станцию о начале сеанса. Сервер также загружает другую информацию при начале сеанса пользователя, как например установки пользователя, свой каталог и переменные среды.

По умолчанию не все учетные карточки в домене позволяют входить в систему. Только карточкам групп администраторов, операторов сервера, операторов управления печатью, операторов управления учетными карточками и операторов управления резервным копированием разрешено это делать.

Для всех пользователей сети предприятия предусмотрено свое имя и пароль.

#### *6.1.3. Учетные карточки пользователей*

Каждый клиент, который использует сеть, должен иметь учетную карточку пользователя в домене сети. Учетная карточка пользователя содержит информацию о пользователе, включающую имя, пароль и ограничения по использованию сети, налагаемые на него. Имеется возможность также сгруппировать пользователей, которые имеют аналогичные ресурсы, в группы; группы облегчают предоставление прав и разрешений на ресурсы, достаточно сделать только одно действие, дающее права или разрешения всей группе.

Таблица 6.1 показывает содержимое учетной карточки пользователя.

Таблица 6.1

Содержимое учетной карточки.

|  |  |  |
| --- | --- | --- |
| Учетная карточка пользователя. | Элемент учетной карточки. | Комментарии. |
| Username  Password  Full name Logon hours | Имя пользователя  Пароль  Полное имя  Часы начала сеанса | Уникальное имя пользователя, выбирается при регистрации.  Пароль пользователя.  Полное имя пользователя.  Часы, в течение которых пользователю позволяется входить в систему. Они влияют на вход в систему сети и доступ к серверу. Так или иначе, пользователь вынужден будет выйти из системы, когда  его часы сеанса, определенные политикой безопасности, истекут |
| Logon workstations  Expiration date | Рабочие станции  Дата истечения срока | Имена рабочих станций, на которых пользователю позволяется работать. По умолчанию пользователь может использовать любую рабочую станцию, но возможно введение ограничений.  Дата в будущем, когда учетную карточку автоматически исключают из базы, полезна при принятии на работу временных служащих |
| Учетная карточка пользователя. | Элемент учетной карточки. | Комментарии. |
| Home directory  Logon script  Profile  Account type | Собственный каталог  Сценарий начала сеанса  Установки (параметры)  Тип учетной карточки | Каталог на сервере, который принадлежит пользователю; пользователь управляет доступом к этому каталогу.  Пакетный или исполняемый файл, который запускается автоматически, когда пользователя начинает сеанс.  Файл, содержащий запись о параметрах среды рабочего стола (Desktop) пользователя, о таких, например, как сетевые соединения, цвета экрана и установочные параметры, определяющие, какие аспекты среды, пользователь может изменить.  Тип учетной карточки - глобальный или локальный. |

#### *6.1.4. Журнал событий безопасности*

Windows 2000 Server позволяет определить, что войдет в ревизию и будет записано в журнал событий безопасности всякий раз, когда выполняются определенные действия или осуществляется доступ к файлам. Элемент ревизии показывает выполненное действие, пользователя, который выполнил его, а также дату и время действия. Это позволяет контролировать как успешные, так и неудачные попытки каких-либо действий.

Журнал событий безопасности для условий предприятиа является обязательным, так как в случае попытки взлома сети можно будет отследить источник.

Таблица 6.2 включает категории событий, которые могут быть выбраны для ревизии, а также события покрываемые каждой категорией.

Таблица 6.2

Категории событий для ревизии.

|  |  |
| --- | --- |
| Категория | События |
| Начало и конец сеанса  Доступ к файлам и объектам | Попытки начала сеанса, попытки конца сеанса; создание и завершение сетевых соединений к серверу  Доступы к каталогу или файлу, которые устанавливаются для ревизии в диспетчере файлов; использование принтера, управление компьютером |
| Использование прав пользователя  Управление пользователями и группами  Изменения полиса безопасности  Перезапуск, выключение и система  Трассировка процесса | Успешное использование прав пользователя и неудачные попытки использовать права, не назначенные пользователям  Создание, удаление и модификация учетных карточек пользователя и групп  Предоставление или отменена прав пользователя пользователям и группам, установка и разрыв связи доверия с другими доменами  Остановка и перезапуск компьютера, заполнение контрольного журнала и отвержение данных проверки если контрольный журнал уже полон  Начало и остановка процессов в компьютере |

Таблица 6.3 показывает типы доступа к каталогам и файлам, которые можно проверить.

Таблица 6.3

Типы доступа к каталогам и файлам.

|  |  |
| --- | --- |
| Доступ к каталогу | Доступ к файлу |
| Отображение имен файлов в каталоге  Отображение атрибутов каталога  Изменение атрибутов каталога | Отображение данных, хранимых в файле  Отображение атрибутов файла  Отображение владельца файла и разрешений |
| Создание подкаталогов и файлов  Переход в подкаталогах каталога  Отображение владельца каталога и разрешений  Удаление каталога  Изменение разрешений каталога  Изменение владельца каталога | Изменение файла  Изменение атрибутов файла  Запуск файла  Удаление файла  Изменение файловых разрешений  Изменение владельца файла |

#### *6.1.5. Права пользователя*

Права пользователя определяют разрешенные типы действий для этого пользователя. Действия, регулируемые правами, включают вход в систему на локальный компьютер, выключение, установку времени, копирование и восстановление файлов сервера и выполнение других задач.

В домене Windows 2000 Server права предоставляются и ограничиваются на уровне домена; если группа находится непосредственно в домене, участники имеют права во всех первичных и резервных контроллерах домена. В каждой рабочей станции Windows 98 и в каждом компьютере Windows 2000 Server, который не является контроллером домена, предоставленные права применяются только к этому единственному компьютеру.

Для каждого пользователя предприятия обязательно устанавливаются свои права доступа к информации, разрешение на копирование и восстановление файлов. [2]

#### *6.1.6. Установка пароля и политика учетных карточек*

Для домена можно определить все аспекты политики пароля: минимальную длину пароля (по умолчанию 6 символов), минимальный и максимальный возраст пароля (по умолчанию устанавливается 14 и 30 дней) и исключительность пароля, который предохраняет пользователя от изменения его пароля на тот пароль, который пользователь использовал недавно (по умолчанию должен предохранить пользователей от повторного использования их последних трех паролей).

Дается возможность также определить и другие аспекты политики учетных карточек:

- должна ли происходить блокировка учетной карточки;

- должны ли пользователи насильно отключаться от сервера по истечении часов начала сеанса;

- должны ли пользователи иметь возможность входа в систему, чтобы изменить свой пароль.

Когда разрешена блокировка учетной карточки, тогда учетная карточка блокируется в случае нескольких безуспешных попыток начала сеанса пользователя, и не более, чем через определенный период времени между любыми двумя безуспешными попытками начала сеанса. Учетные карточки, которые заблокированы, не могут быть использованы для входа в систему. Блокировка учетной карточки обязательно должна быть установлена в предприятие, что бы предотвратить попытки входа в систему.

Если пользователи принудительно отключаются от серверов, когда время его сеанса истекло, то они получают предупреждение как раз перед концом установленного периода сеанса. Если пользователи не отключаются от сети, то сервер произведет отключение принудительно. Однако отключения пользователя от рабочей станции не произойдет. Часы сеанса в фирме устанавливаться не будут, так как в успешной деятельности заинтересованы все сотрудники и зачастую некоторые остаются работать сверхурочно или в выходные дни.

Если от пользователя требуется изменить пароль, то, когда он этого не сделал при просроченном пароле, он не сможет изменить свой пароль. При просрочке пароля пользователь должен обратиться к администратору системы за помощью в изменении пароля, чтобы иметь возможность снова входить в сеть. Если пользователь не входил в систему, а время изменения пароля подошло, то он будет предупрежден о необходимости изменения, как только он будет входить. Изменение своего пароля будет разрешено не для всех пользователей, в компьютерных классах будет запрещено менять пароль, эта возможность будет только у администрации сети.

#### *6.1.7. Шифрованная файловая система EFS*

Windows 2000 предоставляет возможность еще больше защитить зашифрованные файлы и папки на томах NTFS благодаря использованию шифрованной файловой системы EFS (Encrypting File System). При работе в среде Windows 2000 можно работать только с теми томами, на которые есть права доступа. В файловых системах, в которых не используется шифрование, если запускается компьютер по сети или воспользоваться загрузочной дискетой MS DOS или Windows 98, можно получить доступ ко всем файлам, хранящимся на диске, так как на пользователя в этом случае не распространяются ограничения доступа, сведения о которых содержатся в специальных списках контроля доступа.

При использовании шифрованной файловой системы EFS можно файлы и папки, данные которых будут зашифрованы с помощью пары ключей. Любой пользователь, который захочет получить доступ к определенному файлу, должен обладать личным ключом, с помощью которого данные файла будут расшифровываться. Система EFS так же обеспечивает схему защиты файлов в среде Windows 2000. Однако не следует

забывать о том, что при использовании шифрования производительность работы системы снижается.[2]

# Заключение

В аттестационной работе рассмотрены вопросы организации корпоративной сети.

Данная тема имеет немаловажное значение для дальнейшего развития предприятия. На сегодняшний день разработка и внедрение локальных информационных систем является одной из самых интересных и важных задач в области информационных технологий. Появляется потребность в использовании новейших технологий передачи информации. Интенсивное использование информационных технологий уже сейчас является сильнейшим аргументом в конкурентной борьбе, развернувшейся на мировом рынке.

Особое внимание уделено вопросам безопасности и администрирования сети.

В качестве ОС выбрано сервера Windows 2000 Advanced Server, ОС рабочих станций Windows 2000 Рrofessional, т.к. эти ОС наиболее надежны и большее количество современного ПО рассчитано на эти ОС. Кроме ОС Windows 2000 обладает гибкостью, позволяющей расширять, сужать или распределять серверные системы без ущерба для многофункциональности и соотношения цена/быстродействие для платформы операционной системы.

Так же операционная система Windows 2000 предоставляет средства для обеспечения конфиденциальности и целостности данных на следующих уровнях:

* при входе в сеть;
* в локальных сетях и при переходе между сетями;
* при локальном хранении данных.

Сделан также подробный обзор служб Windows 2000 Advanced Server:

Главным отличием Windows 2000 является Active Directory (служба каталогов) — один из наиболее важных компонентов распределенной компьютерной системы. Она решает следующие задачи:

1. Обеспечивает заданную администраторами безопасность для защиты данных от потенциальных нарушителей.
2. Распределяет содержимое каталога по многим компьютерам сети.
3. Реплицирует каталог, чтобы сделать его доступным для большего числа пользователей, а также повысить его отказоустойчивость.
4. Разбивает каталог на разделы по нескольким хранилищам, создавая возможность хранения очень большого числа объектов.

DHCP (Dynamic Host Configuration Protocol) — это стандарт, описан­ный в документах RFC (Request for Comments) и позволяющий DHCP-серверам динамически распределять IP-адреса, а также управлять со­ответствующими параметрами конфигурации протокола IP для сете­вых клиентов, поддерживающих стандарт DHCP. DHCP упрощает и сокращает усилия, затрачиваемые на конфигурирование узлов TCP/IP. Каждый компьютер в сети должен иметь уникальное имя и IP-ад­рес. При его перемещении в другую подсеть необходимо изменить IP-адрес и другие параметры конфигурации. Включение в проект сервера DHCP позволит Вам динамически обновлять конфигурацию клиентов.

DNS сетевая служба разрешения имен, которая позволяет ком­пьютерам сети регистрировать и выполнять прямое и обратное раз­решение доменных имен в IP-адреса. Пользователи и приложения используют доменные DNS-имена для поиска и обращения к ресур­сам, предоставляемым другими компьютерами в корпоративной сети и/или других сетях, например в Интернете.

DNS поддерживает распределенную базу данных для регистрации и обработки запросов *полных доменных имен*.

• DNS-сервер имен, соответствующий требованиям документов RFC;

• поддержка взаимодействия с другими реализациями серверов DNS;

• интеграция со службами Active Directory, WINS и DHCP;

• динамическое обновление зон в соответствии с рекомендациями RFC;

• добавочные зонные передачи между серверами DNS.

WINS поддерживает распределенную базу данных для автомати­ческой регистрации и обработки запросов на разрешение NetBIOS-имен от компьютеров в сети. Включите в проект WINS, если требует­ся разрешение NetBIOS-имен в маршрутизируемой IP-среде.

Служба Routing and Remote Access (Маршрутизация и удаленный до­ступ) поддерживает доступ удаленных пользователей к ресурсам, рас­положенным в частной сети организации. Используйте Routing and Remote Access, когда требуется обеспечить доступ удаленным пользо­вателям — по телефонной линии или по VPN-каналу через Интернет.

Так же в аттестационной работе выбрана оптимальная аппаратная конфигурация сервера и произведен расчет нагрузки спроектированной ЛВС.

# Список использованной литературы

1. Windows 2000 Server. Учебный курс MCSE. – М.: изд-во Русская редакция, 2000. – 612с.
2. Администрирование сети на основе Microsoft Windows 2000. Учебный курс MCSE. – М.: изд-во Русская редакция, 2000. – 512с.
3. Андреев А.Г. Новые технологии Windows 2000 / под ред. А.Н. Чекмарева – СПб.: БХВ – Санкт-Петербург, 1999. – 592с.
4. Вишневский А. Служба каталога Windows 2000. Учебный курс. - СПб.: Питер, 2001. – 464с.
5. Кульгин М. Технология корпоративных сетей. Энциклопедия. – СПб.: Питер, 2001. - 704с.
6. Милославская Н. Г/ Интрасети: доступ в Internet, защита. Учебное пособие для ВУЗов. – М.: ЮНИТИ, 1999 – 468 с.
7. Новиков Ю. Локальные сети: архитектура, алгоритмы, проектирование. – М.: изд-во ЭКОМ, 2000. – 568 с.
8. Норенков И.П., Трудоношин В.А. Телекоммуникационные технологии и сети. - М.: изд-во **МГТУ им. Н.Э.Баумана,** 1999 – 392с.
9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 2-е изд - СПб.: Питер-пресс, 2002 – 864с.
10. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей – СПб.: БХВ – Санкт-Петербург, 2000. – 512с.
11. Разработка инфраструктуры сетевых служб Microsoft Windows 2000. Учебный курс MCSE М.: изд-во Русская редакция, 2001. – 992с.
12. Сосински Б., Дж. Московиц Дж. Windows 2000 Server за 24 часа. – М.: Издательский дом Вильямс, 2000. – 592с.
13. Тейт С. Windows 2000 для системного администратора. Энциклопедия. – СПб.: Питер, 2001. - 768с.