МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к проведению лабораторных работ по дисциплине Анализ и проектирование инфокоммуникационных сетей

для направления 09.04.02 Информационные системы и технологии
профиль Управление данными

Оглавление

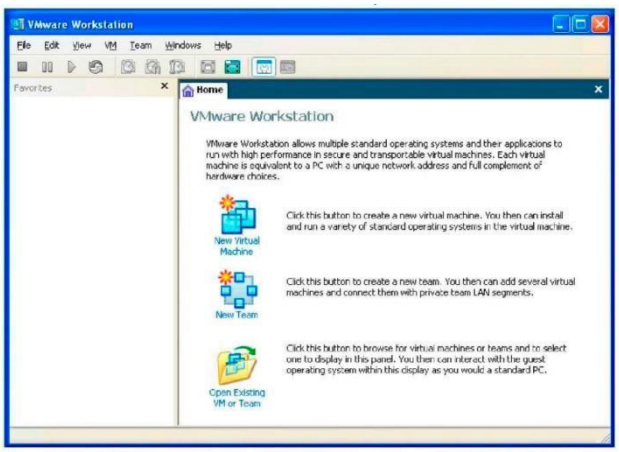
Лабораторная работа №1-2. Организация функционирования ЛВС на базе операционной системы Windows Server. Установка ОС и построение контроллера домена.

Целью данной работы является приобретение навыков установки операционной системы (ОС) Windows Server и настройка сетевых служб ADS (Active Directory Services), DNS (Domain Name Server), DHCP (Dynamic Host Configuration Protocol). Построение Контроллера Домена (Domain Controller).

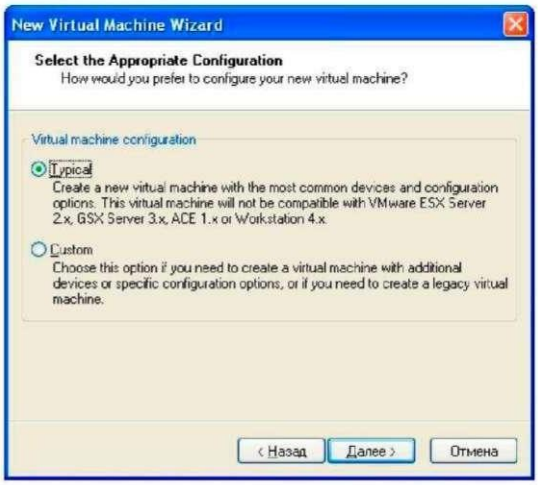
Ход выполнения лабораторной работы.

1. Создание виртуальной машины

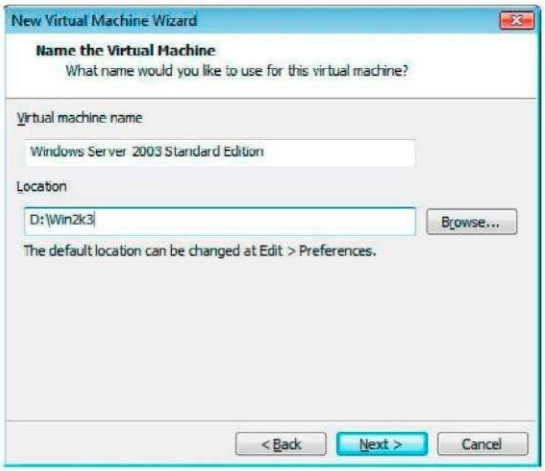
Запустите VMWare Workstation. И выберите «New Virtual Machine»



Следуйте следующим экранам. Нажимаем «Далее». Конфигурацию виртуальной машины уточните у преподавателя.



Выбираем тип и версию операционной системы. В нашем случае «Microsoft Windows» и «Windows Server Standard». Далее вводим наименование и размещение виртуальной машины.



Выбираем тип сетевого соединения для виртуальной машины.

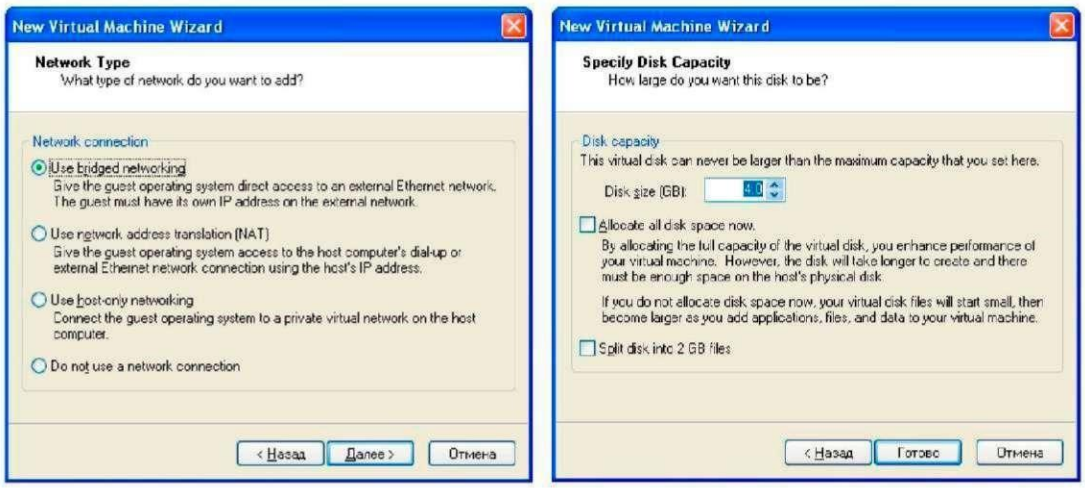
Существует три основных режима подключения виртуальной машины к сети: Bridged mode, NAT и Host Only.

Bridged mode дает виртуальной машине непосредственный доступ к внешнему интерфейсу хост-машины, на котором виртуальная машина самостоятельно устанавливает или получает через DHCP собственные

сетевые параметры - такие как IP-адрес, маршрутизатор по умолчанию и тому подобные.

NAT использует трансляцию адресов исходящего трафика. Напомню, что в этом случае адрес виртуальной машины, полученный по встроенному в NAT DHCP, в момент пересылки на внешний протокол подменяется на адрес хост-машины.

Третий режим **Host Only** представляет дела так, будто у хост-машины в дополнение к имеющимся сетевым интерфейсам есть еще одна сетевая карточка (видимая в системе и без запуска VM), к которой подключается наша ВМ, образуя с хост-машиной маленькую подсеть. Таким образом, можно устроить сеть на одном компьютере.



Выбираем расположение образов операционной системы. Для запуска виртуальной машины нажмите следующий значок

2. Установка операционной системы

Windows Server - это операционная система семейства Windows NT от компании Microsoft, предназначенная для работы на серверах. Она была выпущена 24 апреля 2003 года

Перед нами стоит задача построить сеть из нескольких компьютеров и сделать один из них сервером. Начнем с установки. Мы будем устанавливать

Windows Server. Установка с автозагружающегося CD- диска ничем не отличается от установки Windows. Во время настроек языка (Regional and Language Options) нажмите Customize и в закладке Regional Options, в пункте Standarts and formats выберите Ukraine

(рис. 3.1). То же самое выберите в пункте Location в той же закладке. Далее нажмите закладку Advanced в поле Select a language to match the language version of the non-Unicode programs you want to use и выберите Russian. Тем самым мы обеспечили корректное отображение русского языка в программах, например Far или Total Commander, а также нормальное написание валюты, дат и чисел. Переходим к следующему пункту.

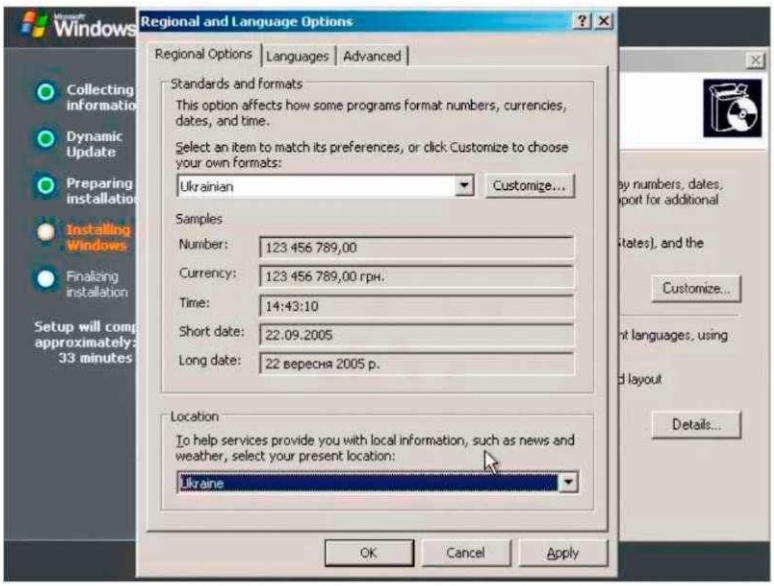


Рисунок 3.1- Выбор языка.

Введя имя и название организации, а также регистрационный ключ, попадаем в Режим лицензирования (Licensing Modes), где вам предложат два варианта: на сервер (Per Server) или же на устройство или пользователя (Per device or Per User) (рис. 3.2)

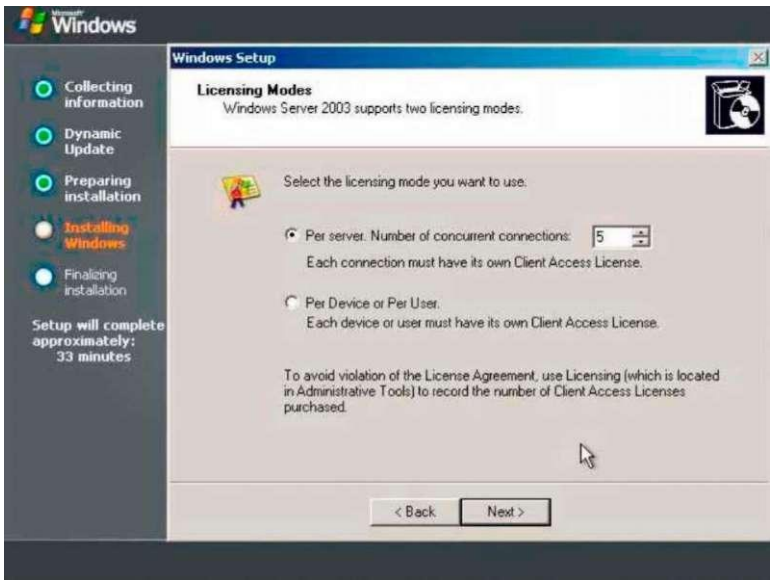


Рисунок 3.2 - Выбор режима лицензирования.

Для настройки сети мы выбираем настройки вручную. Выбираем ***Internet Protocol (TCP/IP),*** кликаем на кнопку ***Properties (Свойства),*** отменяем автоматическое получение IP-адреса, вбиваем 192.168.0.1 в поле ***IP address,*** нажимаем *Tab,* — маска подсети должна автоматически заполниться и принять вид 255.255.255.0 (все остальные поля должны остаться пустыми). Нажав на *Далее,* мы увидим предложение подключить сервер либо к рабочей группе, либо к домену. Ни то, ни другое нам не надо, нажимаем кнопку *Далее* и ждем завершения установки (рис. 3.3).

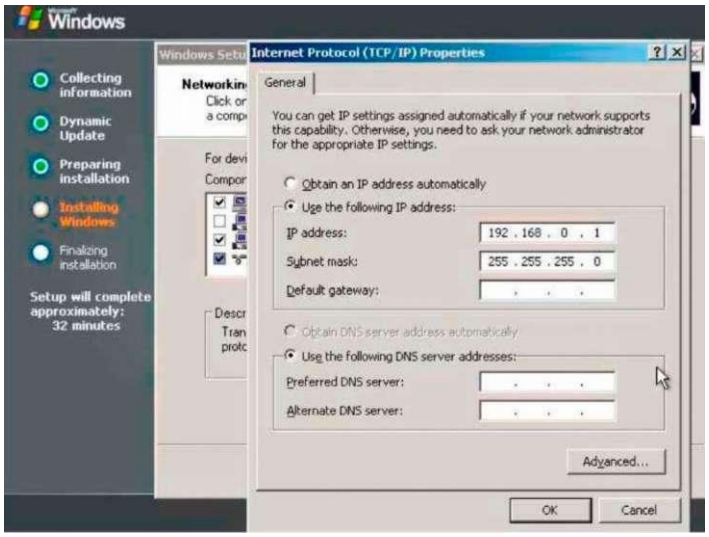


Рисунок 3.3 - Задание IP-адреса.

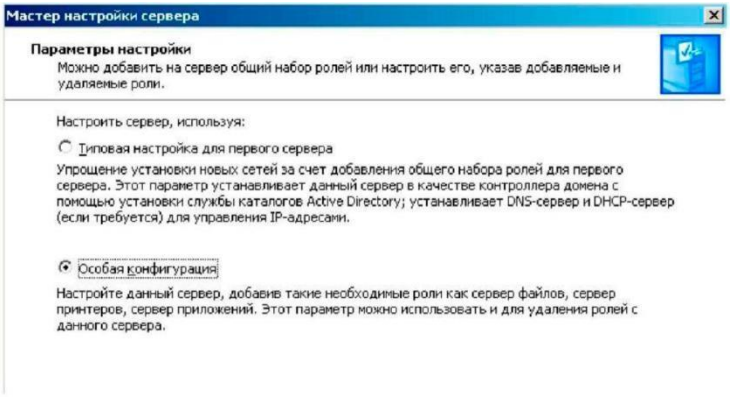
Что такое **маска подсети?** Это число, состоящее из четырех октетов, которые определят, какая часть IP-адреса является сетевым адресом, а какая — адресом хоста. Маска это делает, «маскируя» с помощью двоичного числа часть сетевого IP-адреса, отведенную для нумерации подсетей. Например, IPадрес 207.29.170.193, а маска — 255.255.255.0. Тогда IP-адрес и маска в двоичном виде будут, соответственно, 11001111.11011011.10101010.11000001 и 11111111.11111111.11111111.00000000. Таким образом, все числа, «накрытые» маской, являются номерами подсетей, а последнее десятичное число, или же 8 бит, оставлено для адресов хостов подсети. При организации связей между компьютерами в сети как раз маски и используются для определения того, находится ли целевой хост в той же подсети, что и исходный. Если же он удаленный, т.е. не принадлежит этой подсети, исходный хост пошлет информацию по IP-адресу основного шлюза, который, как вы помните, в сетевой настройке сервера мы оставили пустым. Для определения местоположения целевого хоста компьютер применяет операцию ANDing для IP-адресов и масок обоих хостов. Операция ANDing работает следующим образом: взяв в двоичном виде IP-адрес и маску, сервер сравнивает их, и если в соответствующем разряде адреса и маски стоит 1, то результат будет 1. В противном случае результат — 0. Если результаты ее выполнения равны — оба компьютера находятся в одной подсети.

Domain Name Server (сервер доменных имен) — сервер, содержащий базу данных с именами хостов и сопоставленными им IP-адресами. Таким образом, пользователи сети работают с именами хостов, а DNS уже преобразует их в настоящие IP-адреса. Почему мы его оставили пустым? Потому что сервер как раз и будет выполнять функции DNS. Ну вот, установка подходит к концу, перейдем к настройке сервера.

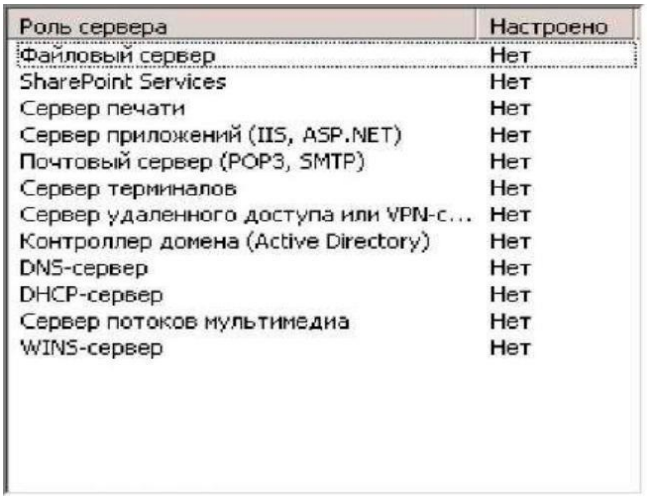
3. Назначение ролей серверу.

Для упрощения дальнейшей нашей работы воспользуемся возможностью ОС **Windows Server** по администрированию сервера, нажимаем *Пуск* (Start) > Управление Вашим Сервером *{Manage Your Server).*

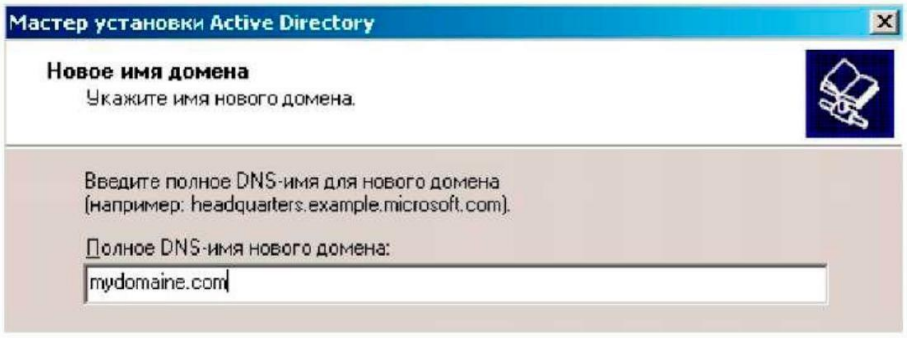
Нажимаем «Новая роль» **(New role),** выбираем «Особая конфигурация» **(Custom** configuration)

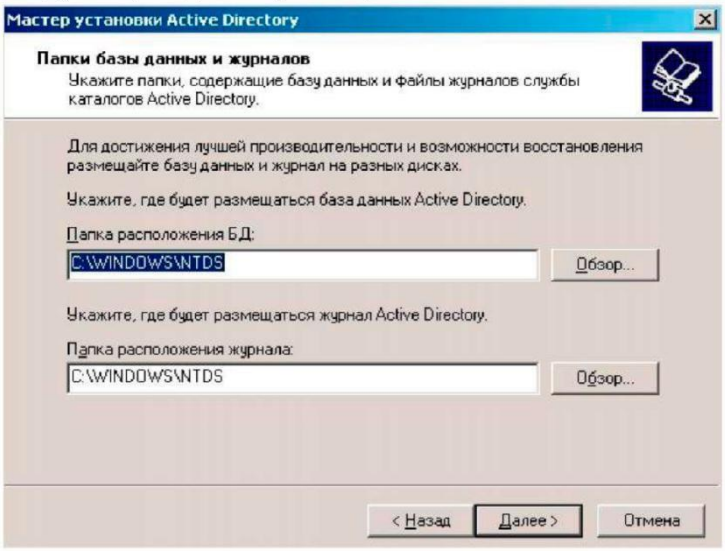


Из списка доступных ролей выбираем «Контроллер домена» **Domain Controller (Active Directory)**



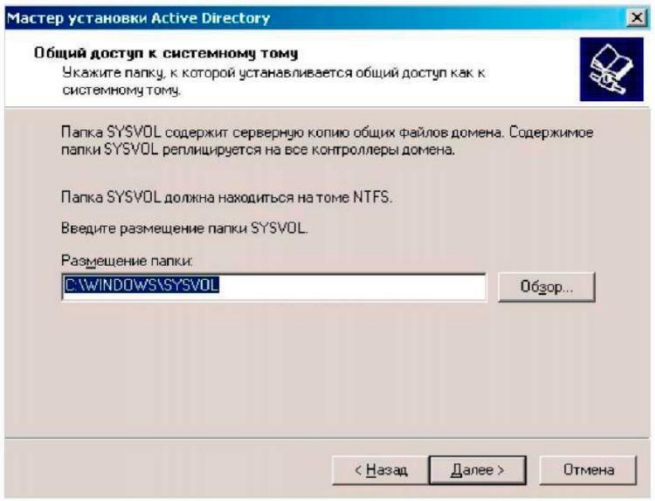
Далее выбираем Контроллер домена в новом домене **(Domain controller for new domain).** Далее опции: «Новый домен в новом лесу» **(Domain in new forest)**





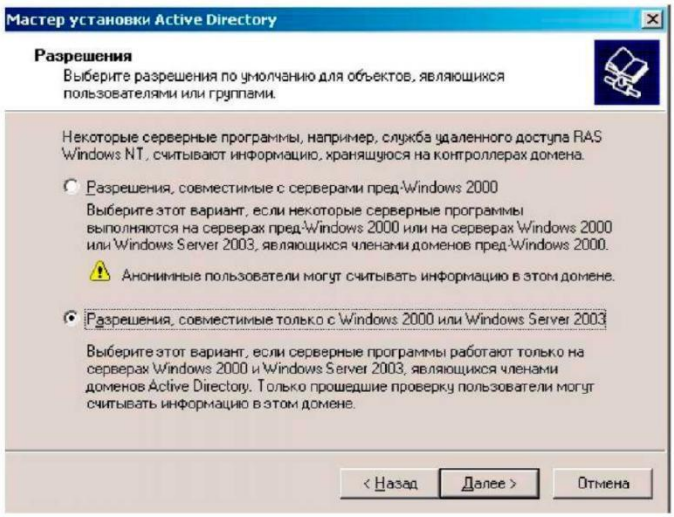
— **NetBIOS name** — MYDOMAINE;

— Следующие две страницы оставляем без изменений;



— Полное DNS-имя нового домена **(Full DNS name)** — mydomaine.com;

Выбираем «Разрешения, совместимые только с Windows или Windows Server» (Permissions compatible with Windows or Windows Server operation systems)



— вводим пароль администратора, перезагружаемся.

Как вы уже поняли, этой последовательностью действий мы сделали наш сервер Контроллером Домена (Domain Controller), а соответственно, «подняли» на нем службу Active Directory и, наконец, настроили DNS на нашем компьютере.

Что такое **активный каталог?** Сети Windows структурируются с помощью служб активного каталога или **ADS** (Active Directory Services). Они

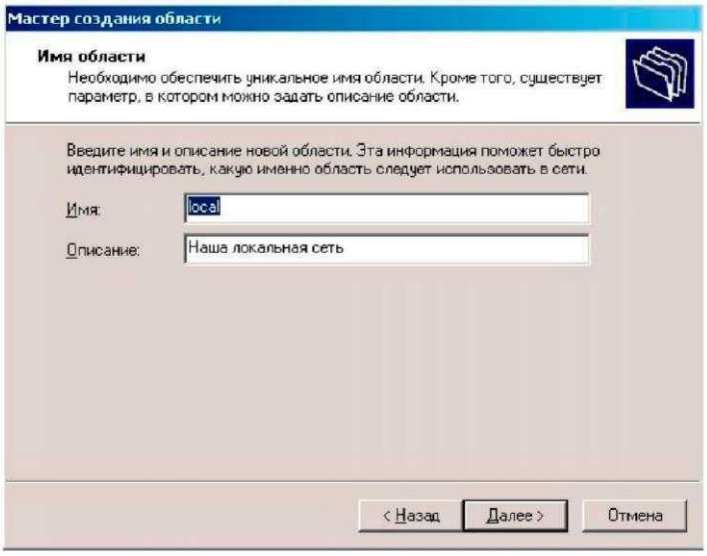
устанавливаются и управляются средствами серверов Windows. Все компоненты компьютерной сети (т.е. компьютеры- пользователи, всевозможные сетевые ресурсы и т.д.) для ADS являются объектами, свойства которых определяются с помощью различных атрибутов. Все объекты, входящие в ADS, образуют каталог. Для удобства управления этими объектами в ADS используются контейнеры, задача которых состоит в хранении остальных объектов, а также в настройке их работы.

Компьютеры могут объединяться в логические единицы, называемые доменами. Каждый домен управляется контроллером домена, хранящим общую для домена информацию и выполняющим общую централизованную авторизацию подсоединившихся пользователей. В отличие от доменов на базе Windows, контроллеров в доменах Windows может быть несколько, и они равноправны. Для еще большего структурирования домены могут объединяться в «деревья».

Ну что ж, мы настроили DNS и ADS. Для легкости в расширении сети, ведь сейчас для того чтобы добавить компьютер в наш домен, нам необходимо выделить вручную ему IP-адрес и каждый раз прописывать маску, основной шлюз, предпочтительный и альтернативный адреса DNS.

Хорошо, если у Вас несколько компьютеров, а если их сотни? И тут на арену выходит **DHCP** (Dynamic Host Configuration Protocol — протокол динамической конфигурации хоста), который, судя по названию, решит все эти проблемы. Давайте его установим и настроим.

В окне *Manage Your Server* нажимаем «Новая роль» **(New role) > DHCP Server,** в окне **Имя области** вводим: *Name:* local.



На следующей странице Start IP-Address: 192.168.0.1; End IP-Address: 192.168.0.100; маска подсети должна принять значение 255.255.255.0, Исключения (Exclusions) пропускаем (если хотите, можете указать диапазон тех адресов, области из которых выбирать нельзя) Длительность: 31 день (период резервирования адреса).

Далее выбираем «Да, я хочу настроить эти опции сейчас», Router (Default Gateway)— 192.168.0.1 (Add), Domain Name and DNS servers — 192.168.0.1 (Add).

WINS Server я оставляю пустым, т.к. сеть у нас на основе Windows, Yes, I want to activate this scope now (Finish).

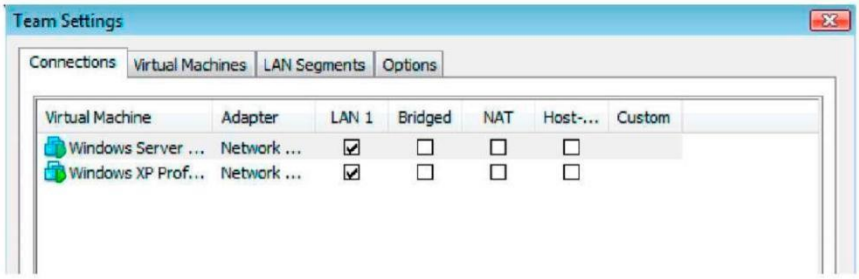
Далее, все в том же окне «Управление Вашим сервером» **(Manage Your Server)** выбираем пункт «Управление DHCP сервером» **(Manage this DHCP server),** откроется окно, именуемое консолью для управления нашего DHCP-сервера. В левой части этого окна выбираем пункт такого вида: имя сервера, название домена [IP-адрес сервера] (в нашем случае: server.mydomaine.com [192.168.0.1]). Теперь в главном меню нажимаем пункт Действия > Авторизировать **(Action > Authorize),** и таким образом мы авторизировали наш DHCP-сервер в сети.

4. Настройка сетевого взаимодействия в VMWare.

Для проверки правильности настройки нашего сервера необходимо организовать сетевое взаимодействие сервера с клиентами. В качестве клиента возьмем предварительно установленный образ «Windows XP».

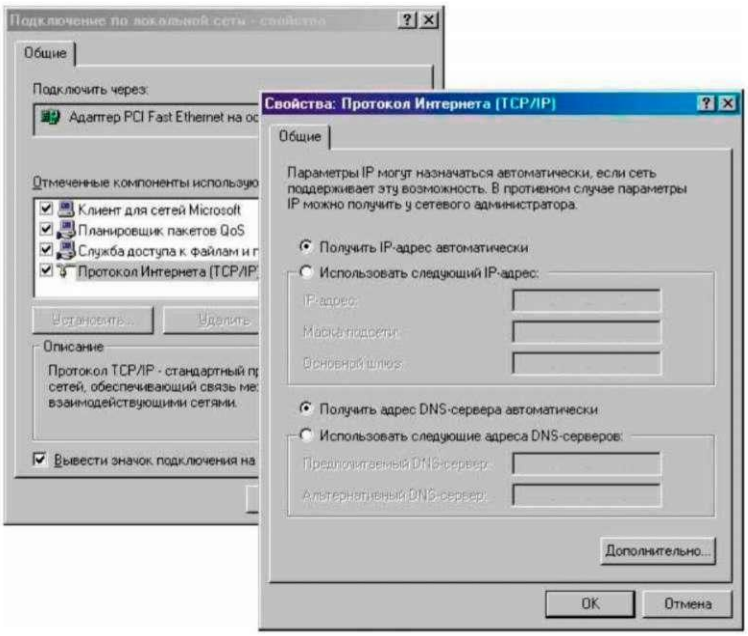
Выполним следующие действия:

1. Завершим работу с серверной и клиентской ОС. Выполним команду «Отключить питание» (Power Off).
2. Создадим новую команду (Team). Выполним File>New>Team.
3. Добавим наши операционные системы (Server) в команду.
4. Настроим сетевые параметры



5. Добавление клиентских машин в домен.

На клиентском компьютере выбираем Пуск> Настройка > Сеть и удаленный доступ к сети, кликаем правой кнопкой мыши на Подключение по локальной сети, выбираем Свойства, затем Протокол Интернета (TCP/IP), опять же Свойства. Выбираем Получить IP-адрес автоматически.



Далее, нажав правой кнопкой мыши по иконке «Мой компьютер», выбираем *Свойства > Имя компьютера > Изменить.* В пункте *«Является членом* выбираем *домена»* и вводим выбранное имя домена (MYDOMAINE) и нажимаем ОК. Выведется окно с запросом имени и пароля пользователя, который имеет соответствующие права для подключения компьютера в домен.

Вывод. Установив Windows Server и настроив некоторые службы, Вы познакомились с огромным миром серверных технологий. Это было лишь поверхностное ознакомление, на следующих занятиях мы изучим более детально возможности данной ОС.

Контрольные вопросы

1. Что такое контроллер домена?
2. Для чего предназначена служба DNS?
3. Почему у сервера DNS должен быть статический IP- адрес?
4. Для чего предназначен протокол DHCP?
5. Назовите необходимые действия и их порядок для добавления клиентской машины в домен.

Лабораторная работа №3-4. Организация функционирования ЛВС на базе операционной системы Windows Server. Управление учетными записями пользователей.

Целью данной работы является приобретение навыков управления учетными записями пользователей, а также их профилями.

Условием работы любой сети, конечно же, является наличие в ней пользователей и компьютеров. Сегодня мы изучим возможности по созданию пользователей в глобальном каталоге Active Directory и попробуем управлять компьютерами и пользователями в нашей ЛВС.

Ход выполнения лабораторной работы.

1. Подготовка хранилища профилей пользователей.

Прежде чем мы перейдем к созданию пользователей нашего домена, необходимо выполнить несколько предварительных действий. Во-первых, необходимо определить, где будут храниться профиля пользователей. Пусть у нас это будет папка «Profiles» на диске С. После создания этой папки необходимо открыть к ней общий доступ (рис. 5.1) и дать разрешение всем на чтение и изменение (кнопка Разрешение, рис. 5.2).

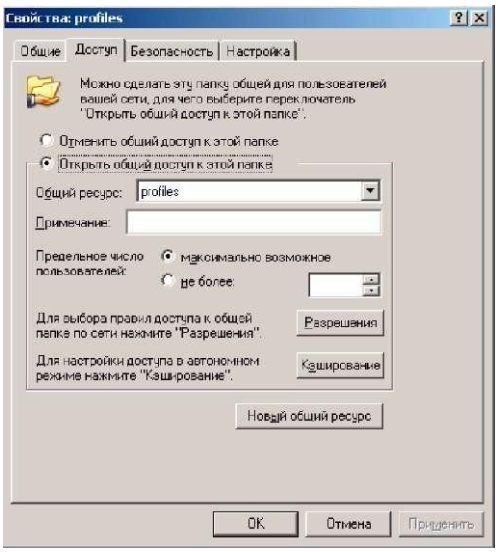


Рисунок 5.1

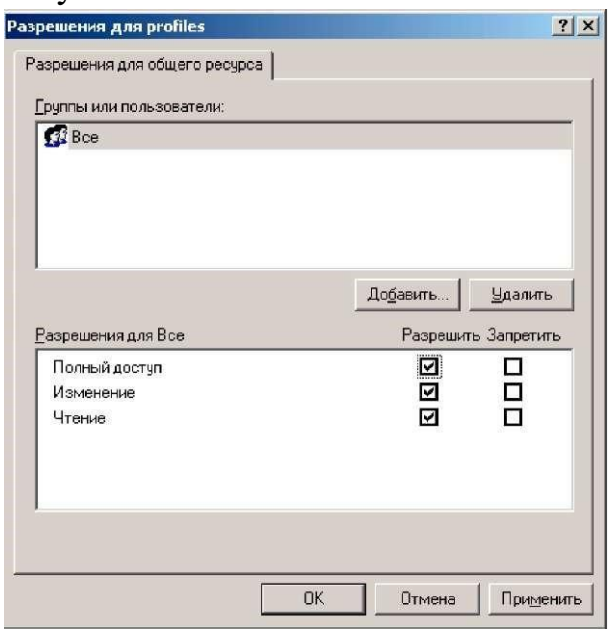


Рисунок 5.2

2. Создание пользователей

Для управления сервером воспользуемся консолью mmc. Нажмите Пуск\Выполнить... (Start\Run...), в текстовом поле введите mmc и нажмите [Enter]. Откроется окно (рис. 5.3), озаглавленное «Консоль» («Consolel»). Нажимаем Консоль\Добавить или удалить оснастку (File\Add/Remove Snap-In), дальше выбираем Добавить (Add) и из списка предложенных инструментов добавляем в список только необходимые. Это делается путем нажатия на кнопку Добавить (Add). Нажмите Закрыть\ОК (Close\Ok) — и Вы получите несколько открытых элементов управления в одном окне. Дальше консоль можно сохранить и открывать уже настроенную. Таким образом, все необходимые инструменты будут всегда находиться у Вас под рукой.

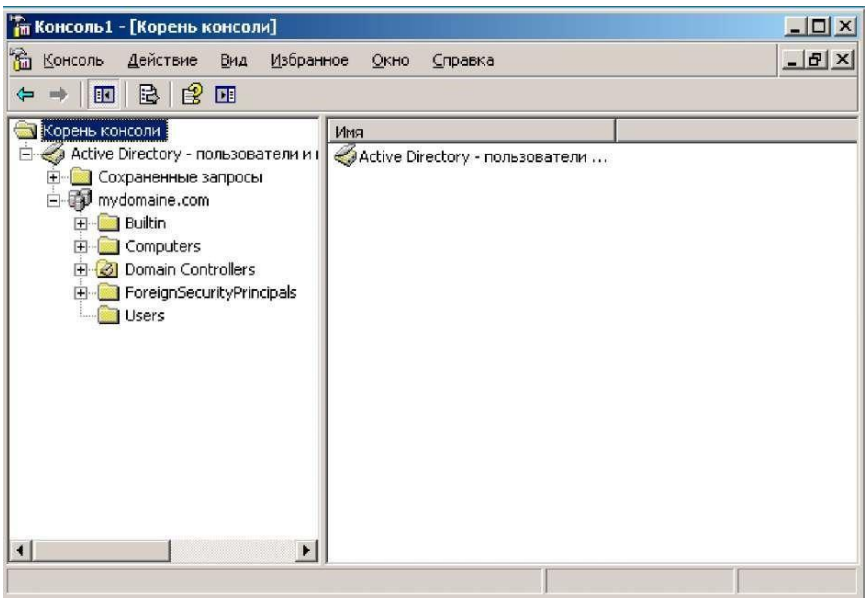


Рисунок 5.3.

Теперь перейдем непосредственно к созданию первых пользователей. В отличие от компьютеров, которые автоматически добавляются при их подключении к серверу, создавать пользователей придется вручную. Сразу замечу, что лучше сразу же организовывать каталог так, чтобы пользователи и компьютеры не размещались в стандартных контейнерах (Organisation Unit), а каким-то образом систематизировались.

Итак, создадим первого пользователя и поместим его не в стандартном контейнере Users, а в подразделении. Нажимаем правой кнопкой мыши на названии домена в оснастке *«Active Directory Users and Computers»,* выбираем *Создать\Подразделение,* вбиваем название «MyDepartment» и жмем ОК.

Далее выбираем в меню Действие (Action) пункт Создать\Пользователь (New\User) создаем нового пользователя (эти действия эквивалентны нажатию правой кнопки мыши на контейнере и выбору пункта Создать\Пользователь (New\User)). Откроется диалоговое окно «Новый объект — Пользователь» (New Object — User). На его первой странице нам будет необходимо ввести сведения об имени пользователя **(рис. 5.4).**

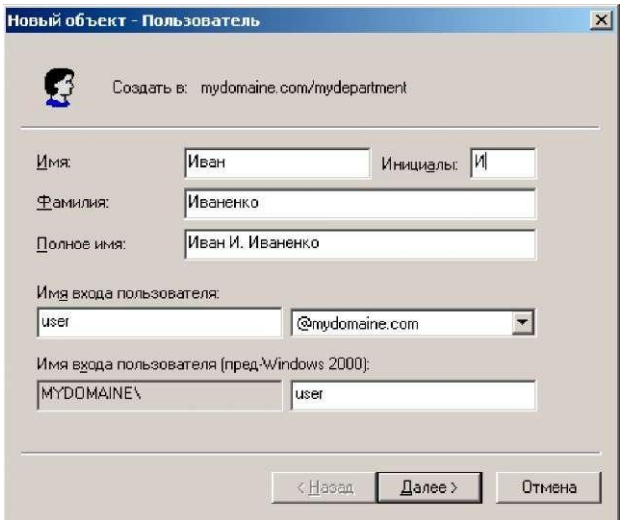


Рисунок 5.4.

Закончив ввод значений и щелкнув *Далее (Next),* мы увидим вторую страницу, на которой надо будет ввести пароль пользователя, введем «password».

Здесь также необходимо установить настройки данной учетной записи. Остановимся на них подробнее:

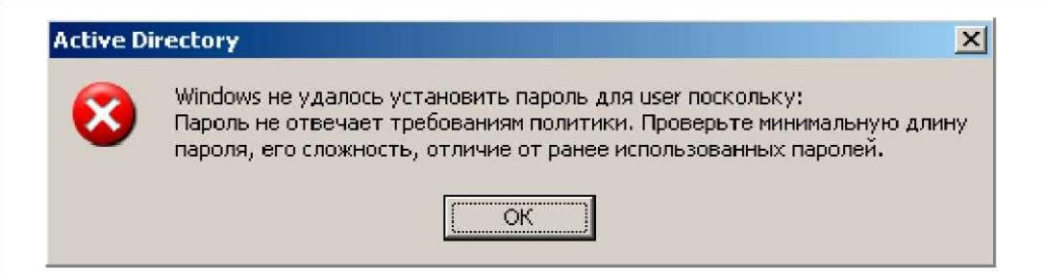
- Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon) — установлено по умолчанию. Очень удобное средство для того, чтобы пароль пользователя знал только он. Вы создаете учетную запись, например, со стандартным паролем Microsoft (p@s$w0rd) и требуете, чтобы пользователь изменил его сразу же при запуске системы. Пользователь просто не войдет в систему, не изменив пароль!
- Запретить смену пароля пользователя (User Cannot Change Password)

— установите этот флажок, если этой учетной записью пользуются несколько пользователей в домене (в частности, это касается учетной записи Гость (Guest), ведь если какой-то пользователь случайно изменит пароль, то доступ

к системе будет невозможен для остальных пользователей, использующих учетную запись.

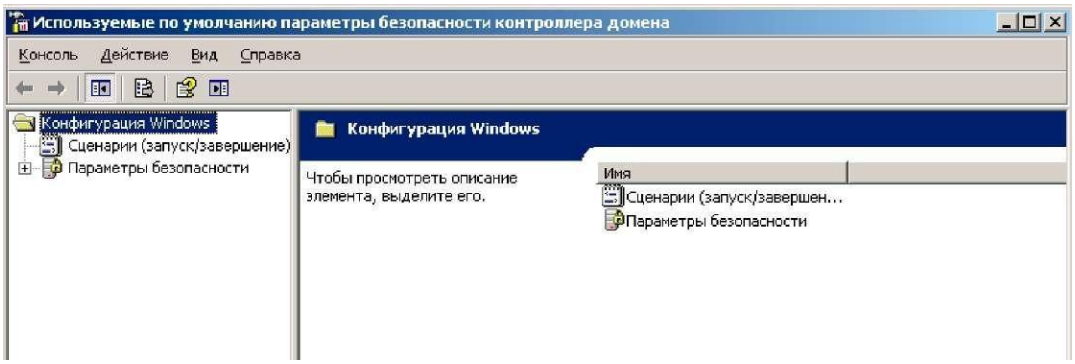
- Срок действия пароля неограничен (Password Never Expires) — используйте этот флаг для не очень защищенных сетей (вроде домашней, которую мы и строим). В защищенных его обязательно надо снимать, т.к. пароли пользователей, имеющих доступ к конфиденциальной информации, должны меняться регулярно.
- Отключить учетную запись (Account is disabled) — для создания пользователей, которым пока нет необходимости входить в сеть.

Нажав *Далее\Готово (Next\Finish),* мы заканчиваем создание нового пользователя в каталоге Active Directory, но скорее всего Вы получите следующие сообщение.

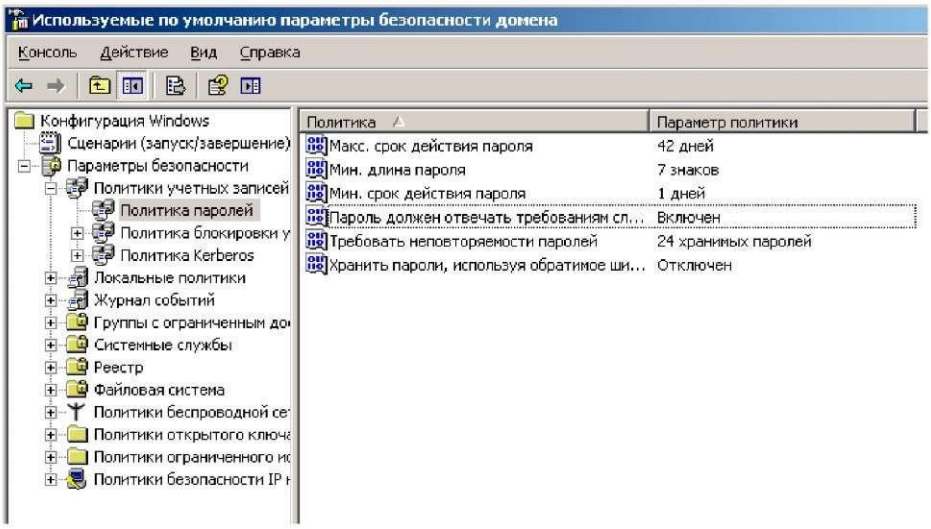


Проблема заключается в том, что пароль, который Вы ввели не отвечает требованиям безопасности. У нас есть два пути: вводить сложный пароль (более 7 знаков и содержать буквы в разных регистрах и цифры) или изменить текущую политику безопасности.

Нажмите Пуск > Администрирование > Политика безопасности домена

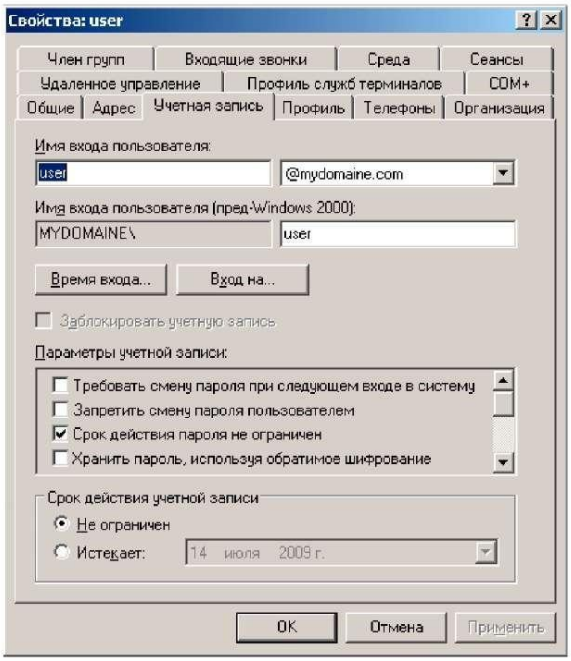


Параметры безопасности - Политика учетных записей - Политика паролей.



После создания пользователя, теперь мы вполне можете просмотреть его свойства, выбрав в меню Действие (Action) пункт Свойства (Properties). Перед Вами откроется диалоговое окно, в котором находится весь спектр информации об этом пользователе. Особое внимание стоит обратить на закладку Учетная запись (Account) — рис. 5.5.

Рисунок 5.5.



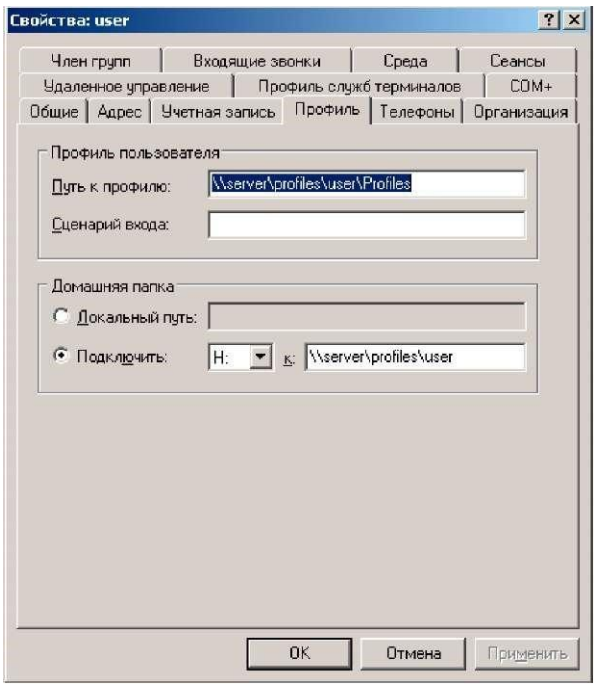


Рисунок 5.6.

Определенные свойства были уже настроены при создании пользователя. Рассмотрим назначение некоторых из них:

- Время входа (Logon Hours) — позволяет настроить время, когда пользователю позволено входить в сеть.
- Вход на (Log On To) — определение компьютеров, с которых пользователю позволено входить в домен.

- Хранить пароль, используя обратимое шифрование (Store Password Using Reversible Encryption) — этот параметр разрешает хранение пароля в Active Directory без использования мощного алгоритма для шифрования

хешированием (между прочим — без возможности обратного преобразования!). Используется для поддержки приложений, которым требуется знать пароль пользователя. Пользуйтесь этим параметром только в случае крайней необходимости, т.к. это существенно ослабляет безопасность (пароли, которые хранятся с использованием обратимого шифрования, для опытного взломщика — практически то же самое, что и пароль, записанный в блокноте открытым текстом).

- Срок действия учетной записи (Account Expires) — позволяет задать дату окончания действия учетной записи.

На рис.5.6 размещены настройки расположения профиля пользователя и домашняя папка пользователя. У нас это папка «Profiles» на диске «C» (см. выше).

Можно также одновременно менять некоторые свойства у нескольких учетных записей. Для этого надо выделить нужные учетные записи и выбрать их свойства.

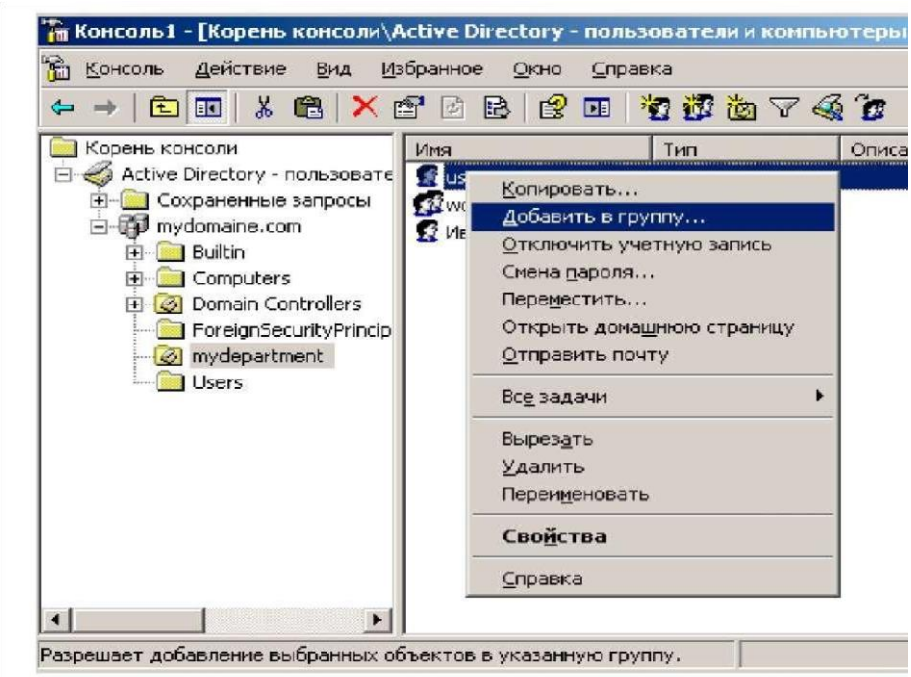
Перейдем к понятию **Групп.** Группы — это контейнеры, которые содержат объекты пользователей и компьютеров. Если в разрешениях к доступу к файлам и папкам заданы группы, то эти права распространяются на всех членов этой группы. Чтобы создать группу, выберите контейнер, щелкните правой кнопкой мыши и выберите пункт *Создать\Группа (New\Group).* Затем вы сможете задать тип и область действия создаваемой группы.

Группы бывают двух типов: группы безопасности и группы распространения. *Группы безопасности* (security groups) используются для назначения доступа к сетевым ресурсам, в то время как *группы распространения* (distribution groups) применяются для объединения пользователей в списки рассылки электронной почты. Как Вы наверняка догадались, нам необходимо создавать группы именно первого типа.

Область действия группы определяет, каким образом ее составу назначаются разрешения в доступе. Здесь Вам следует выбрать одну из трех областей:

- Локальная доменная (Domain local) — используется для назначения группам разрешений на доступ к локальным ресурсам домена.
- Глобальная (Global) — эти группы часто применяются для объединения пользователей или компьютеров в одном домене и совместного исполнения одной и той же работы, какой-либо роли или функции.
- Универсальная (Universal) — из такой области применяют преимущественно для предоставления доступа к ресурсам во всех доверенных доменах.

В основном Вам необходимо будет использовать группы с областью действия Domain local.



Сетевые ресурсы

Для создания сетевого ресурса на сервере необходимо:

1. Определится с расположением ресурса, и создать папку.
2. Отдать ресурс в общий доступ (рис. 5.7).
3. Дать разрешение на ресурс определенным группам и пользователям (рис.5.8).

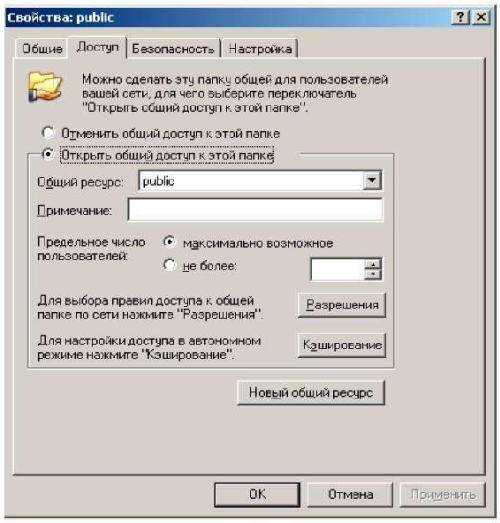


Рисунок 5.7.

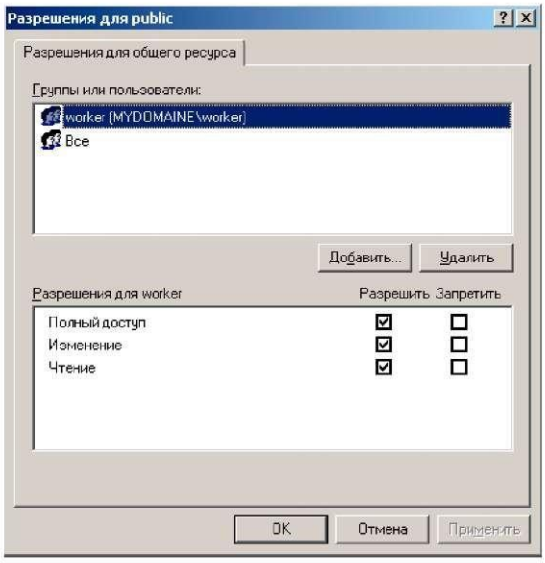


Рисунок 5.8.

Ход выполнения лабораторной работы. Часть вторая.

В ходе работы необходимо изучить теоретические сведенья, связанные с администрированием пользователей, а также проделать практические задания и ответить на контрольные вопросы, описанные ниже.

1. Создать подразделение **«enterprise»:**

2. Создать следующие группы в данном подразделении:
-workers,

-teachers, -students.

3. Создать пользователей user_[номер варианта]_ N, где N =1, 2, .., 5.

Пользователей с N равным 1 и 2 добавить в группу workers.

Пользователей с N равным 3, 4 и 5 добавить в группу students.

4. Создать пользователя teacher_[номер варианта].

Имя учетной записи должна содержать Ваше ФИО.

Пользователя добавить в группу teachers.

5. Для всех пользователей user_[номер варианта]_ N задайте пароли «password». Для пользователя teacher_[номер варианта]

6. Создать директорию labs в корневом каталоге. В нем создать каталоги library и tests

7. Создать файлы book_[фамилия студента] и поместить их в library

8. Дать право на изменение файла только пользователю teacher_[номер варианта], а на чтение пользователям группы workers.

9. Настроить права доступа к каталогу library и tests, таким образом, чтобы пользователи группы teachers могли изменять и создавать там файлы, а пользователи группы students имели доступ на чтение и при входе в домен автоматически подключались эти директории как диски «L» и «T» соответственно.

10. Проверьте всю проделанную работу, войдя под всеми созданными Вами пользователями из клиентской ОС в домен «MYDOMAINE».

Вывод. В результате проделанной лабораторной работы Вы должны были приобрести базовые навыки управления доступом к сетевым ресурсам, а также добавления новых пользователей (групп) в сеть.

Контрольные вопросы:

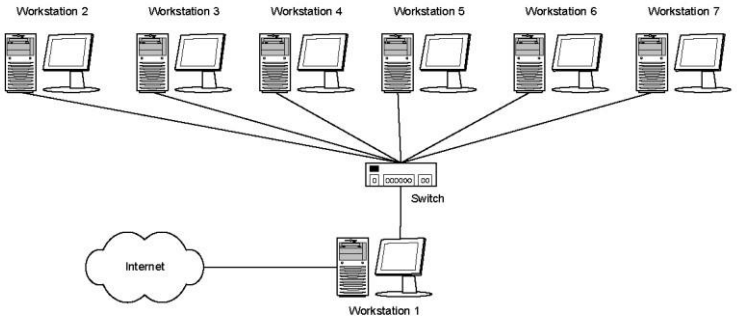
1. Что такое профиль пользователя?
2. Для чего нужны группы пользователей?
3. Почему при создании нового пользователя возникала ошибка при использовании пароля «password»?
4. Какие действия необходимо выполнить для создания нового пользователя?
5. Каким образом автоматизировать подключение сетевого диска?

Лабораторная работа №5-6. Настройка доступа к сети Интернет из локальной сети.

Цель работы: Рассмотреть различные варианты подключения к сети Интернет локальной сети, использую различные программные средства.

Дано: Имеется локальная сеть (***Workstantion 1 - Workstantion 2)*** представленная на рисунке. На компьютере (шлюзе), через который планируется подключение локальной сети к Internet необходимо наличие двух сетевых адаптеров (подключений).

Задание: Необходимо обеспечить доступ к сети Интернет со всех рабочих станций.



Краткие теоретические сведенья:

Имеются три основных варианта подключения локальной сети к Интернет:

1. «прямое» IP-подключение,
2. подключение через NAT,
3. подключение через прокси-сервер.

Рассмотрим преимущества, недостатки и область применения каждого метода, а также некоторые возникающие нюансы. Выбор конкретного способа подключения зависит от потребностей пользователей, цели подключения и, в некоторой степени, финансовых возможностей.

Итак, компьютер ***Workstantion 1.*** У него есть доступ, как к Интернету, так и к локальной сети. Наша задача - дать компьютерам локальной сети

доступ к Интернет через подключенный к нему компьютер. Далее этот компьютер мы будем называть шлюзом или маршрутизатором.

Рассмотрение способов мы начнем с наименее часто использующегося, наиболее дорогого, но также наиболее «правильного» и естественного способа, дающего наибольшие по сравнению с другими способами возможности.

«Прямое» IP-подключение к Internet. Для того, чтобы Ваша локальная сеть была полноценно подключена к Интернету, должны соблюдаться, как минимум, три условия:

1. Каждая машина в локальной сети должна иметь "реальный", интернетовский IP-адрес;
2. Эти адреса должны быть не любыми, а выделенными Вашим провайдером для Вашей локальной сети (скорее всего, это будет подсеть класса C);
3. На компьютере-шлюзе, подключенном к двум сетям - локальной сети и сети провайдера, должна быть организована IP-маршрутизация, т.е. передача пакетов из одной сети в другую.

В этом случае Ваша локальная сеть становится как бы частью Интернета. Собственно, это тот способ подключения, которым подключены к Интернету сами Интернет-провайдеры и хостинг-провайдеры.

В отличие от обычного подключения, рассчитанного на один компьютер, при таком подключении "под клиента" выделяется не один IP-адрес, а несколько, так называемая "IP-подсеть".

При таком способе подключения Вы можете организовать в своей сети сервисы, доступные из Интернета - ведь при данном подключении не только Интернет полностью доступен из Вашей сети, но и Ваша сеть - из Интернета, т.к. является его частью.

Однако такая "прозрачность" Вашей сети резко снижает ее защищенность - ведь любые сервисы в локальной сети, даже предназначенные для "внутреннего" использования, станут доступными извне через Интернет. Чтобы это не имело места, доступ в локальную сеть извне несколько ограничивают. Обычно это делается установкой на шлюзе программы-firewall. Это своеобразный фильтр пакетов, проходящих из одной сети в другую. Путем его настройки можно запретить вход-выход из локальной сети пакетов, соответствующих определенным критериям - типу

IP-пакета, IP-адресу назначения, TCP/UDP-порту и т.п. Firewall

решает такие задачи, как:

- блокировку доступа извне к определенным TCP/IP-сервисам локальной сети.
- блокировку доступа к определенным компьютерам локальной сети. Таким образом, можно запретить доступ извне ко всем машинам, кроме определенных серверов, предназначенных для доступа из Интернет.
- защиту от троянских программ на сетевом уровне.

Несмотря на универсальность такого метода

подключения локальной сети к Интернет, этот метод имеет недостатки. Благодаря им, его реально и используют только лишь те организации, которым надо сделать свои сервера доступными из Интернет - в основном, те же интернетпровайдеры и хостинг-провайдеры, а также информационные службы. Самый главный недостаток заключается в дороговизне выделения IP-адресов и уж тем более IP-подсетей, к тому же эту плату надо вносить периодически.

Поэтому на практике рассмотрим другие, описанные далее способы, не требующие больших затрат и, что самое главное, позволяющие подключить локальную сеть через обычное подключение с одним внешним IP-адресом.

Подключение через NAT (IP-маскарадинг).

Технология Network Address Translation (NAT) - "трансляция сетевых адресов" позволяет нескольким машинам локальной сети иметь доступ к Интернет через одно подключение и один реальный внешний IP-адрес.

Для того, чтобы компьютера локальной сети могли устанавливать соединения с серверами сети Интернет, нужно, чтобы:

- IP-пакеты, адресованные серверу в Интернет, смогли его достигнуть;
- ответные IP-пакеты, идущие от сервера Интернет на машину в локальной сети, также смогли ее достигнуть.

С первым условием проблем не возникает, а как быть со вторым? Ведь компьютера локальной сети не имеют своего "реального" интернетовского IP-адреса! Как же они могут получать IP-пакеты из Интернет?!

А работает это следующим образом - на компьютере-шлюзе стоит программа NAT-сервера. Компьютер-шлюз прописан на машинах локальной сети как "основной шлюз", и на него поступают все пакеты, идущие в Интернет (не адресованные самой локальной сети). Перед передачей этих IP-пакетов в Интернет NAT-сервер заменяет в них IP-адрес отправителя на свой, одновременно запоминая у себя, с какой машины локальной сети пришел этот IP-пакет. Когда приходит ответный пакет (на адрес шлюза, конечно), NAT определяет, на какую машину локальной сети его надо направить. Затем в полученном пакете меняется адрес получателя на адрес нужной машины, и пакет доставляется этой машине через локальную сеть.

Как видим, работа NAT-сервера прозрачна для машин локальной сети (как и работа обычного IP-маршрутизатора). Единственным принципиальным ограничением этого метода подключения локальной сети к Internet является невозможность установить _входящее_ TCP-соединение из Интернет на машину локальной сети. Однако для "клиентских" сетей этот недостаток превращается в достоинство, резко увеличивающее (по сравнению с первым

методом подключения) их защищенность и безопасность. Администраторы некоторых провайдеров даже употребляют слова NAT и Firewall как синонимы.

Подключение через прокси-сервер.

Это самый простой тип подключения. При этом никакой маршрутизации IP-пакетов между локальной сетью и сетью Интернет не происходит. Машины локальной сети работают с Интернет через программу-посредник, так называемый прокси-сервер, установленный на компьютере-шлюзе.

Основной особенностью этого метода является его "непрозрачность". Если, скажем, в случае NAT программа-клиент просто обращается к Интернет-серверу, не "задумываясь", в какой сети и через какую маршрутизацию она работает, то в случае работы через прокси-сервер программа должна явно обращаться к прокси-серверу. Мало того, клиентская программа должна уметь работать через прокси-сервер. Однако проблем с этим не возникает - все современные и не очень броузеры умеют работать через прокси-сервера.

Другой особенностью является то, что прокси-сервер работает на более высоком уровне, чем, скажем, NAT. Здесь уже обмен с Internet идет не на уровне маршрутизации пакетов, а на уровне работы по конктретным прикладным протоколам (HTTP, FTP, POP3...). Соответственно для каждого протокола, по которым должны «уметь» работать машины локальной сети, на шлюзе должен работать свой прокси-сервер.

Эта «протокольная зависимость» и есть основной недостаток этого метода подключения как самостоятельного.

Почти каждый интернет-провайдер имеет один или несколько прокси-серверов, через которые рекомендует работать своим клиентам. Несмотря на

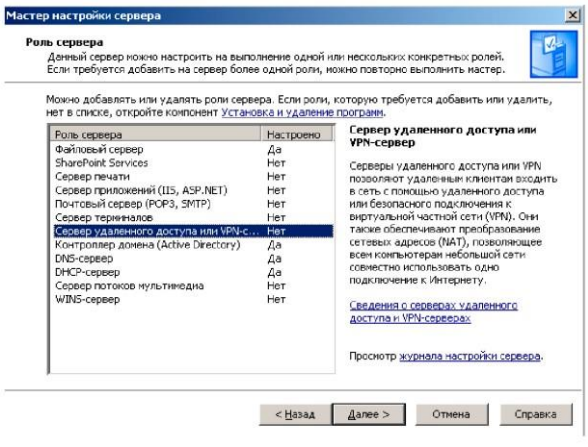
то, что это совершенно необязательно (как правило, клиент провайдера может обращаться к Интернет напрямую), это дает выигрыш в производительности, а при повременной оплате, соответственно, экономить время он-лайн. Это происходит потому, что прокси-сервера способны кэшировать (запоминать) запрашиваемые пользователем документы, и при следующих к ним обращениях выдавать копию из кэша, что быстрее, чем повторно запрашивать с интернет-сервера. Кроме того, прокси-сервера могут быть настроены так, что будут блокировать загрузку баннеров наиболее распространенных баннерных служб, тем самым также (порой значительно) ускоряя загрузку веб-страниц.

При установке HTTP прокси сервера в локальной сети и работе через него за счет кэширования экономится не только время, но и трафик - потому, что кэширование происходит в самой локальной сети, "до" канала с провайдером, в котором считается трафик (при оплате за объем перекачанной информации).

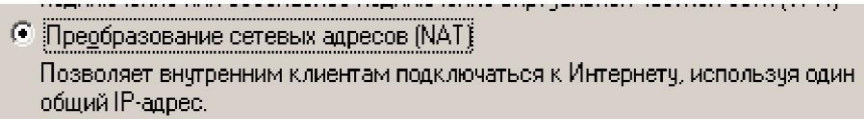
Ход выполнения лабораторной работы. Часть вторая. Настройка подключения через WinServer. NAT

Для создания условий, заданных в лабораторной работе, необходимо выполнить ряд действий:

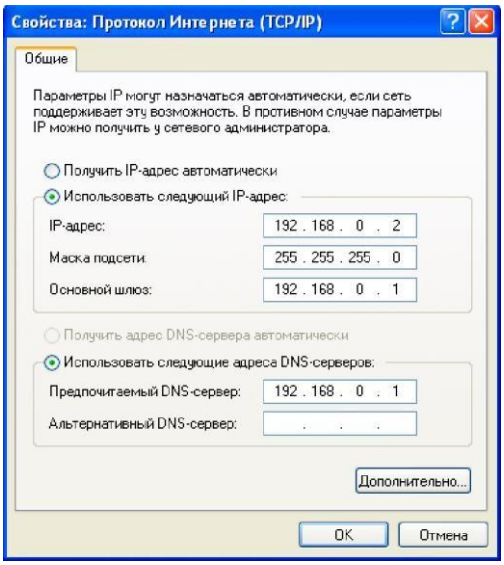
1. Добавляем для WinServer сетевой адаптер, который подключаем по схеме «NAT». Второй подключаем к «LAN1»
2. После загрузки WinServer настраиваем новый сетевой адаптер на автоматическое получение IP- адреса.

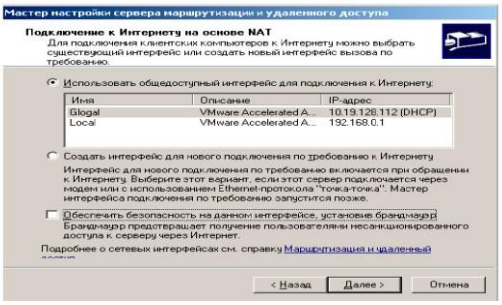


3. Проверяем доступ к Интернет.
4. Запустите режим управления сервером 5. Выберите добавить новую роль.
   6. В списке ролей выберите следующий пункт.
   7. Выберите вариант «NAT»



   8. Выберите интерфейс подключенный к Интернет





   9. Отключите брандмауэр
   10. Введите следующие параметры на клиентской машине

Проверьте работоспособность NAT при помощи команд (с клиентской машины):

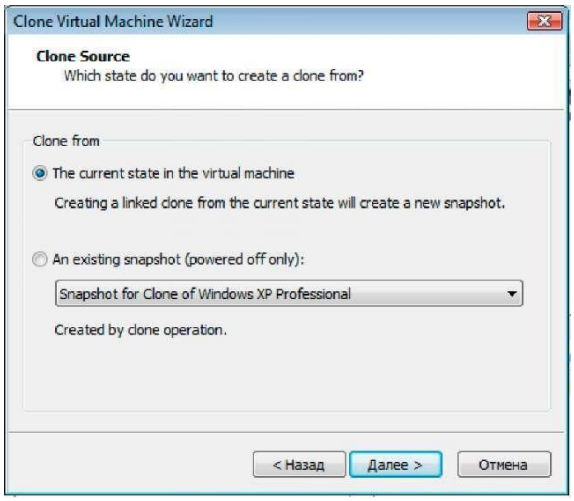
ping 192.168.0.1

ping [адрес адаптера сервера, подключенного к Интернет] Настройка подключения через WinXP. Internet Connection Sharing.

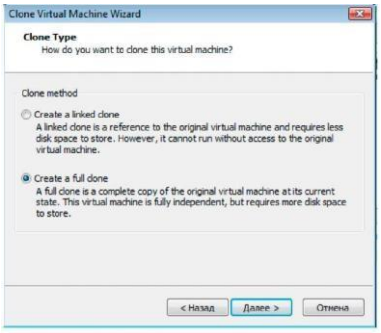
Для выполнения следующих двух этапов необходимо проделать следующие действия:

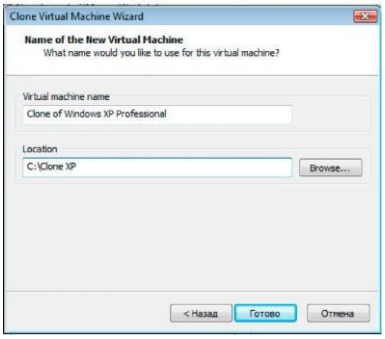
Выключите WinServer и удалите его из Вашей группы.

Создайте клон WinXP.



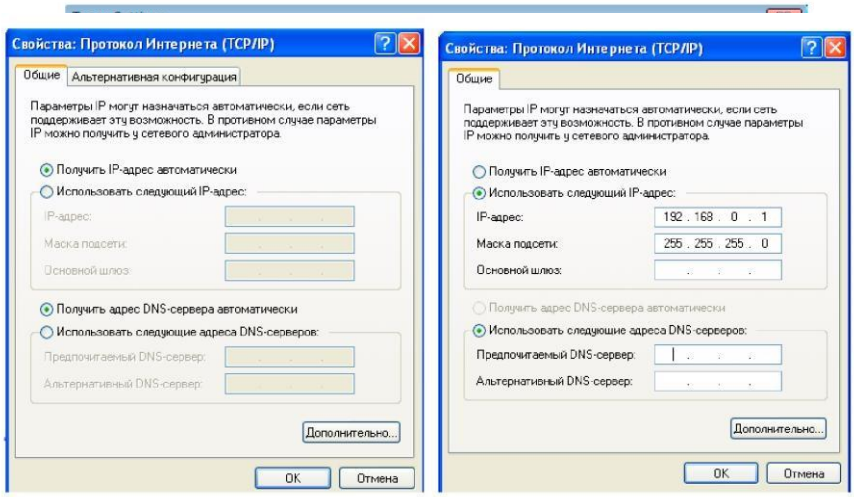
Выполняйте действия согласно рисункам





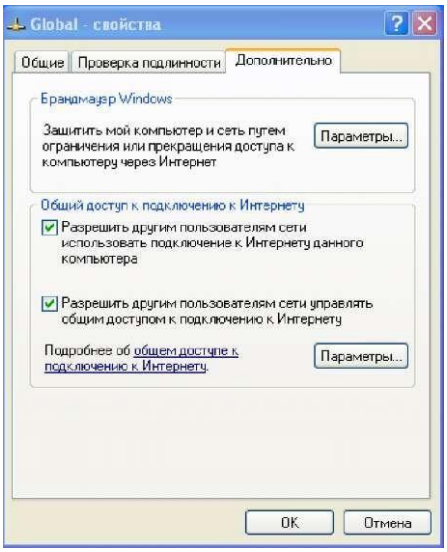
Добавьте новую ОС в группу.
Добавить сетевой адаптер, как показано на рисунке.

Запустить виртуальные машины. Настройте на шлюзе адаптеры, как показано на рисунке.

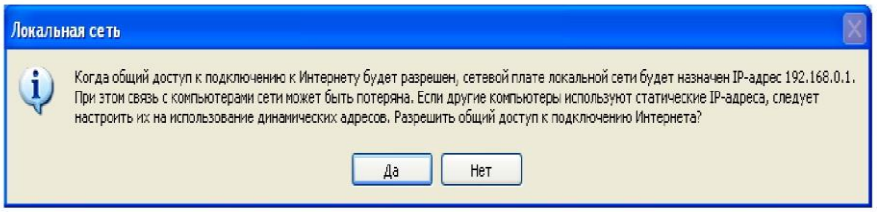


Для удобства переименуйте их

На шлюзе, открываем Панель управления > Сеть и удаленный доступ к сети (Control Panel > Network Connections), выберите ваше подключение правой кнопкой и нажмите Свойства (Properties). В закладке Дополнительно (Advanced) отметьте флажок Общий доступ в моей сети для этого подключения (Allow Other Network Users To Connect Thought This Computer's Internet Connection).



ICS жестко сконфигурирован и назначает компьютеру, обеспечивающему доступ, статический внутренний адрес 192.168.0.1. Все клиенты размещаются в одной физической подсети, получают адреса из диапазона 192.168.0.0/24 (/24 означает первые 24 единицы в маске сети, представленной в двоичной форме, т.е. это маска 255.255.255.0) и используют для разрешения имен только DNS-сервер, размещенный на этом же компьютере.

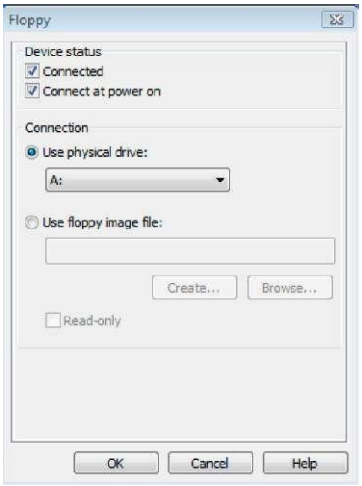


На клиентских машинах устанавливаем Автоматическое получение IP-адреса.

Настройка подключения через WinXP. Прокси-сервер

В качестве прокси-сервера будем использовать **HandyCache (HC)** - это бесплатная программа, которая экономит трафик, ускоряет загрузку страниц, блокирует рекламу и позволяет в автономном режиме (без подключения к Интернет) просмотреть любые посещенные ранее сайты.

На первом этапе необходимо установить прокси сервер на компьютере подключенном к сети Интернет. Используйте дискету или флешку для переноса программы.



Установите и настройте программу. Настройки можете найти на официальном сайте системы http://handycache.ru в разделе Главная ->Документация ->Описание и настройка HandyCache.

Минимальные настройки:

- *Безусловные прокси* - proxy.mipk.kharkiv.edu:8080;
- Список пользователей - *IP-адреса клиентов;*
- Настройка браузера на клиентах.

Вывод. В результате проделанной работы вы должны получить навыки, которые позволят вам подключить локальную сеть к сети Internet, а также организовать совместный доступ к ее ресурсам.

Лабораторная работа №7-8. Механизмы резервного копирования данных в операционной системе Windows Server.

Цель работы: Получить навыки архивирования и восстановления системы, используя стандартные утилиты Windows Server. Решить задачи сетевого администратора связанные с сохранением, архивированием информации, и ее последующим восстановлением.

Дано: Имеется локальная сеть с контроллером домена на базе ОС Windows Server.

Задание: Необходимо, используя стандартные утилиты Windows Server обеспечить архивирование и восстановления системы, а также настроить механизмы резервирования важных данных.

Краткие теоретические сведенья.

Ни один носитель информации не является абсолютно надежным, из строя может выйти любое устройство хранения данных, и данные могут быть потеряны. Кроме аппаратных сбоев возможна также потеря данных по причине действия вредоносных программ (вирусы и т.п.). А самая распространенная причина порчи или удаления данных — ошибки пользователей (как обычных, так и администраторов), которые могут по ошибке удалить или перезаписать не тот файл.

По этой причине возникает необходимость регулярного создания резервных копий информации — файлов с документами, баз данных и состояния операционной системы.

Системы семейства Windows Server имеют встроенный инструмент создания резервных копий — утилиту *ntbackup*. Данная утилита позволяет сохранять резервные копии на самых различных носителях — ленточных накопителях, магнитооптических дисках, жестких дисках (как на локальных дисках данного сервера, так и на сетевых ресурсах, размещенных на других компьютерах сети). В версии системы Windows реализован механизм т.н. теневых копий *Shadow Copy,* который заключается в том, что в начале процедуры архивации система делает моментальный «снимок» архивируемых файлов и уже после этого создает резервную копию из этого снимка. Данная

технология позволяет архивировать файлы, которые в момент запуска утилиты *ntbackup* были открыты пользователями.

Сетевой администратор должен совместно с пользователями определить те данные, которые нужно регулярно архивировать, спланировать ресурсы, необходимые для создания резервных копий, составить расписание резервного копирования, настроить программу резервного копирования и планировщик заданий для автоматического создания резервных копий. Кроме этого, в задачу сетевого администратора входит также регулярное тестирование резервных копий и пробное восстановление данных из резервных копий (чтобы вовремя обнаружить возникающие проблемы в создании резервных копий).

Архивирование и восстановление файловых ресурсов. Базовые понятия службы резервного копирования.

Все операции по созданию резервных копий и восстановлению данных в ОС семейства Windows осуществляются утилитой *ntbackup.*

Рассмотрим основы резервного копирования файловых ресурсов. Каждый файл, хранящийся на диске компьютера, независимо от типа файловой системы, имеет атрибут *archive,* который в Свойствах файла отображается как *«Файл готов для архивирования»* (откройте Свойства файла и нажмите кнопку *«Другие»).* Если в Свойствах файла вручную убрать галочку у этого атрибута, то при любом изменении в файле операционная система автоматически снова установит этот атрибут. На использовании изменений данного атрибута основаны все используемые в системе Windows методики резервного копирования.

Типы резервного копирования.

Утилитой *ntbackup* можно создавать резервные копии различных типов. Рассмотрим их отличительные особенности и различные варианты их применения.

Обычный (Normal)

При выполнении данного типа архивирования утилита *ntbackup* архивирует все файлы, отмеченные для архивации, при этом у всех заархивированных файлов очищается атрибут «Файл готов для архивирования». Данный вид архивирования необходим для создания еженедельных полных резервных копий каких-либо больших файловых ресурсов. Если в компании или организации имеются достаточные ресурсы, то можно ежедневно осуществлять полное архивирование данных.

Разностный (Differential)

При выполнении Разностного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут не очищается. Использование Обычного и Разностного архивирования позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Например, если раз в неделю (как правило, в выходные дни) создавать Обычные копии, а в течение недели ежедневно (как правило, в ночное время) — Разностные, то получается выигрыш в объеме носителей для резервного копирования. При такой комбинации архивирования «Обычный + Разностный» процесс восстановления данных в случае утери информации потребует выполнения двух операций восстановления — сначала из последней Полной копии, а затем из последней Разностной резервной копии.

Добавочный (Incremental)

При выполнении Добавочного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых

установлен атрибут «Файл готов для архивирования», при этом данный атрибут очищается. Использование Обычного (раз в неделю по выходным) и Добавочного (ежедневно в рабочие дни) архивирования также позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Но процесс восстановления данных при использовании комбинации «Обычный + Добавочный» уже будет выполняться иначе: в случае утери информации для восстановления данных потребуется сначала восстановить данные из последней Полной копии, а затем последовательно из всех Добавочных копий, созданных после Полной копии.

Копирующий (Copy)

При таком типе архивирования утилита *ntbackup* заархивирует все отмеченные файлы, при этом атрибут «Файл готов для архивирования» остается без изменений.

Ежедневный (Daily)

Ежедневный тип архивирования создает резервные копии только тех файлов, которые были модифицированы в день создания резервной копии.

Два последних типа не используются для создания регулярных резервных копий. Их удобно применять в тех случаях, когда с какой-либо целью нужно сделать копию файловых ресурсов, но при этом нельзя нарушать настроенные регулярные процедуры архивирования.

Разработка и реализация стратегии резервного копирования. Понятие плана архивации.

Создание и реализация плана архивации и восстановления информации — непростая задача. Сетевому администратору надо определить, какие данные требуют архивации, как часто проводить архивацию и т. д.

При создании плана ответьте на следующие вопросы:

- Насколько важны данные? Этот критерий поможет решить, как, когда и какую информацию архивировать. Для критичной информации, например, баз данных, следует создавать избыточные архивные наборы, охватывающие несколько периодов архивации. Для менее важной информации, например, для текущих пользовательских файлов, сложный план архивации не нужен, достаточно регулярно сохранять их и уметь легко восстанавливать.
- К какому типу относится архивируемая информация? Тип информации поможет определить необходимость архивации данных: как и когда данные должны быть сохранены.
- Как часто изменяются данные? Частота изменения влияет на выбор частоты архивирования. Например, ежедневно меняющиеся данные необходимо сохранять каждый день.
- Нужно ли дополнить архивацию созданием теневых копий? При этом следует помнить, что теневая копия — это дополнение к архивации, но ни в коем случае не ее замена.
- Как быстро нужно восстанавливать данные? Время — важный фактор при создании плана архивации. В критичных к скорости системах нужно проводить восстановление очень быстро.
- Какое оборудование оптимально для архивации и есть ли оно у вас? Для своевременной архивации вам понадобится несколько архивирующих устройств и несколько наборов носителей. Аппаратные средства архивации включают ленточные накопители (это наименее дорогой, но и самый медленный тип носителя), оптические диски и съемные дисковые накопители.
- Кто отвечает за выполнение плана архивации и восстановления данных? В идеале и за разработку плана, и собственно за архивацию и восстановление должен отвечать один человек.

- Какое время оптимально для архивации? Архивация в период наименьшей загрузки системы пройдет быстрее, но не всегда возможно провести ее в удобные часы. Поэтому с особой тщательностью архивируйте ключевые данные.
- Нужно ли сохранять архивы вне офиса? Хранение архивов вне офиса - важный фактор на случай стихийного бедствия. Вместе с архивами сохраните и копии ПО для установки или переустановки ОС.

Для построения правильной и эффективной системы резервного копирования необходимо детально изучить и задокументировать все файловые ресурсы, используемые в компании, а затем тщательно спланировать стратегию резервного копирования и реализовать ее в системе. Для планирования стратегии необходимо ответить на следующие вопросы:

- какие именно ресурсы будут архивироваться;
- минимальный промежуток времени для восстановления данного ресурса при возникновении аварии;
- какой объем данных будет архивироваться;
- какова емкость носителей для хранения резервных копий и скорость записи на эти носители;
- сколько времени будет занимать архивирование каждого ресурса;
- как часто будет производиться архивация каждого ресурса;
- если резервные копии записываются на ленты, то как часто будет производиться перезапись лент;
- по какому графику будет производиться тестовое восстановление данных.

При ответе на эти вопросы будет спланирована потребность в количестве и емкости накопителей и устройств для выполнения резервных копий, требования к пропускной способности сети для создания резервных

копий, график выполнения резервного копирования, план восстановления на случай аварии.

Выбор архивных устройств и носителей.

Определив, какие данные и как часто архивировать, можно выбрать аппаратные средства архивации и необходимые носители. Инструментов для архивации данных множество. Одни быстрые и дорогие, другие — медленные и надежные. Выбор подходящего оборудования для организации зависит от многих факторов.

- Емкость - количество регулярно архивируемых данных. Справится ли оборудование с нагрузкой в отведенное время?
- Надежность аппаратных средств и носителей. Можете ли вы пожертвовать надежностью ради экономии или скорости?
- Расширяемость решения. Удовлетворяет ли ваше решение потребностям роста организации?
- Скорость архивации и восстановления. Можете ли вы пожертвовать скоростью ради снижения стоимости?
- Цена архивации. Приемлема ли она для вашего бюджета?

Типовые решения архивации.

Итак, на план архивации влияют емкость, надежность, расширяемость, скорость и цена. Определив, какие из этих факторов наиболее важны для вашей организации, вы примете подходящее решение. Вот некоторые общие рекомендации:

- Ленточные накопители — самые распространенные устройства архивации. Данные хранятся на кассетах с магнитной лентой. Лента относительно недорога, но не особенно надежна: она может помяться или

растянуться, с течением времени — размагнититься и перестать считываться. Средняя емкость кассет с лентой варьируется от единиц до десятков Гбайт. По сравнению с другими решениями ленточные накопители довольно медленны. Их достоинство — невысокая цена.

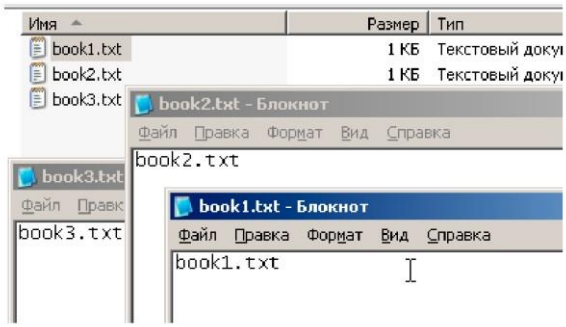
- Накопители на цифровой ленте (digital audio tape, DAT) — пришли на смену традиционным ленточным накопителям. Существует несколько форматов DAT, их емкости составляют 35 и 260 Гбайт.
- Ленточная библиотека с автозагрузкой — устройство для создания расширенных архивных томов на нескольких лентах, которых хватает для нужд всего предприятия. Ленты набора в процессе архивации или восстановления данных автоматически меняются. В большинстве таких библиотек применяются DAT-ленты. Их главный *«минус»* — высокая цена.
- Магнитооптические накопители с автозагрузкой подобны ленточным библиотекам, только вместо лент в них используются магнитооптические диски. Цена также очень высока.
- Съемные диски, например Iomega Jazz емкостью 1-2 Гбайт, все чаще используются в качестве устройств архивации. Они обладают хорошей скоростью и удобны в работе, но стоят дороже ленточных или DAT-накопителей.
- Дисковые накопители обеспечивают наивысшую скорость при архивации и восстановлении файлов. Если при архивации на ленту вам потребуются часы, то дисковый накопитель позволяет завершить процесс за несколько минут. К недостаткам дисковых накопителей следует отнести относительно высокую цену.

Ход выполнения лабораторной работы.

Создания задания на выполнения архивации данных:

1. Создать на диске «С» Вашего сервера каталог *backup* и *restore;*

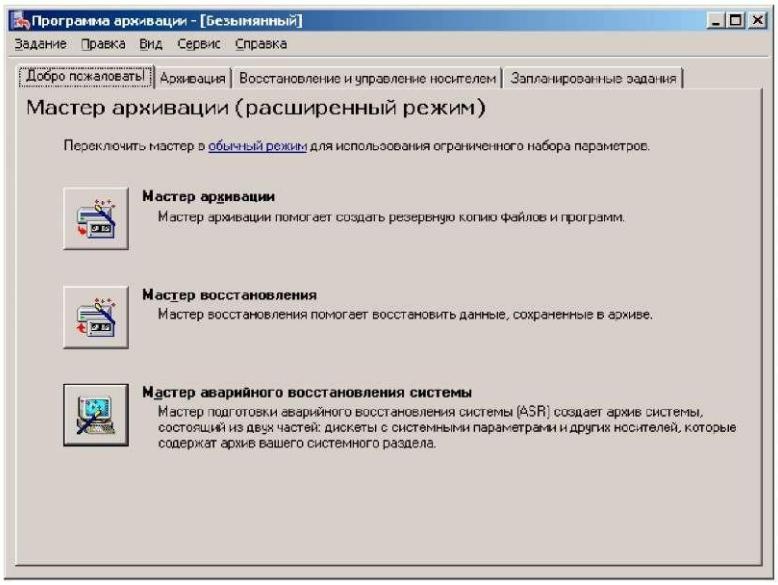
2. В папке library, созданной в одной из предыдущих работ создать 3 текстовых файла с наименованиями *book1.txt, book2.txt* и *book3.txt.* Файлы должны содержать свое наименование.



3. Запустить утилиту резервного копирования *ntbackup.*

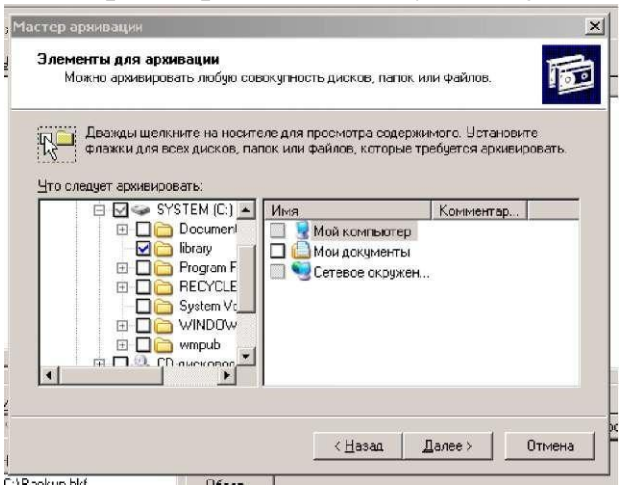
Эту утилиту можно запустить из Главного меню системы (кнопка «Пуск» — «Все программы» — «Стандартные» — «Служебные» — «Архивация данных»), а можно запустить более быстро из командной строки (кнопка «Пуск» — «Выполнить» — «ntbackup» — кнопка «ОК»). При первом запуске утилиты рекомендуем убрать галочку у поля «Всегда запускать в режиме мастера».

4. Запустить «Мастер архивации» (на закладке «Добро пожаловать» нажать кнопку «Мастер архивации».

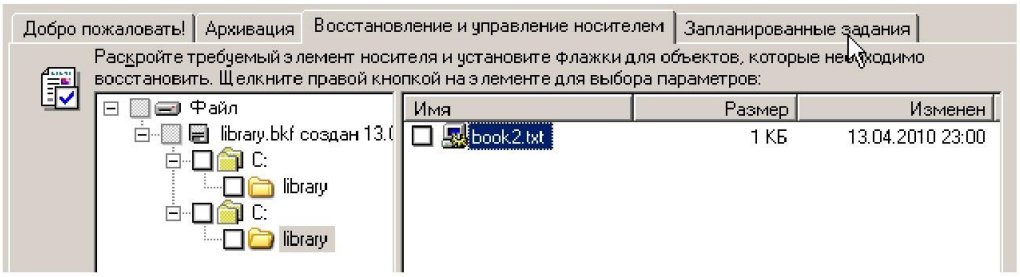


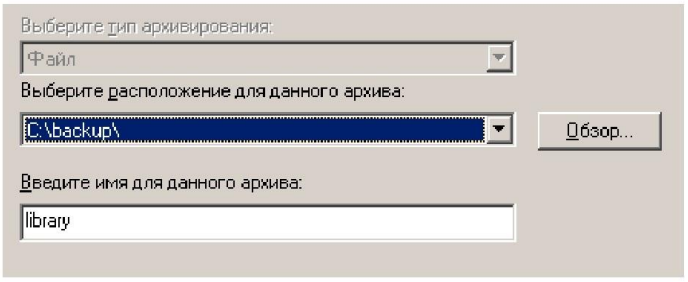
5. После запуска мастера нажмем кнопку «Далее» и выберем, что нам нужно архивировать, в данном примере — «Архивировать выбранные файлы, диски или сетевые данные»

6. Выберем для архивирования папку *library.*

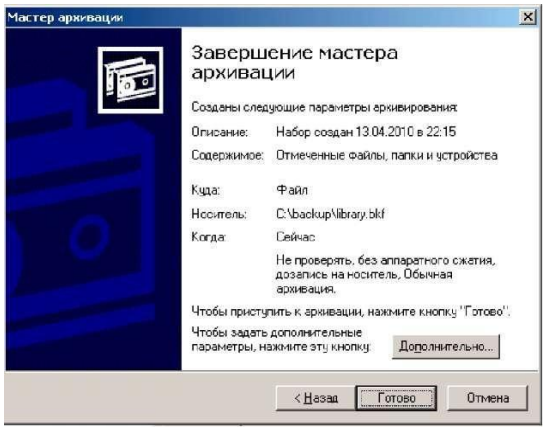


7. *Выберем* место для создания резервной копии, создадим файл с именем *library*, этому файлу автоматически будет назначено расширение *«.bkf»*.

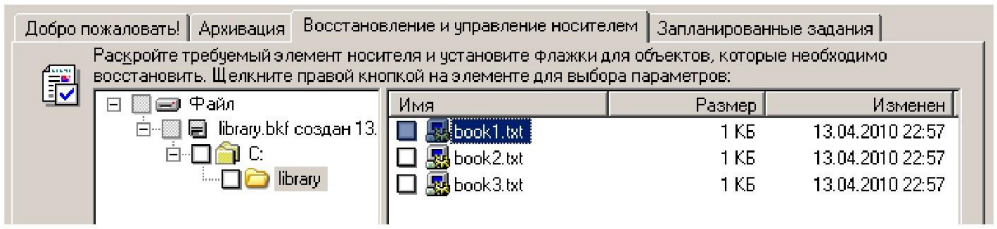




8. На данном этапе нажмем кнопку «Готово».



9. Проверяем полученный результат.



10. Вносим изменение в файл *book1.txt* и *book2.txt*, у файла *book1.txt* убираем атрибут «Файл готов для архивирования», а *book3.txt* - удаляем.

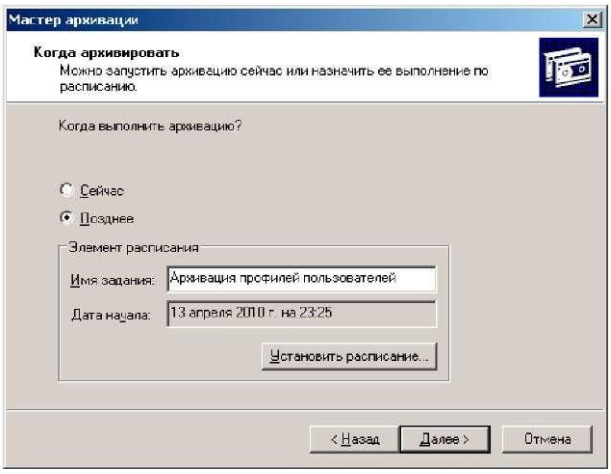
11. Запускаем снова процесс архивации, но на 8 этапе нажмем кнопку «Дополнительно», чтобы задать дополнительные параметры и выбираем тип архивации «Добавочный». Далее все пункты по умолчанию, но при этом не забывайте запоминать, что Вы делаете. Проверяем полученный результат.

12. Восстановите файл *book3.txt.* Для этого выполните следующие действия:

- Запустим утилиту резервного копирования *ntbackup.*
- Перейдем на закладку "Восстановление и управление носителем".
- После появления в списке архивных файлов нужного архива раскроем этот архив и выберем файлы для восстановления из резервной копии. При этом мы можем восстановить файлы в то место, где они были ранее ("Исходное размещение") или выбрать иной путь для их сохранения ("Альтернативное размещение"). Выберите папку *restore.*
- После определения всех параметров восстановления нажмем кнопку "Восстановить", утерянные данные будут восстановлены.

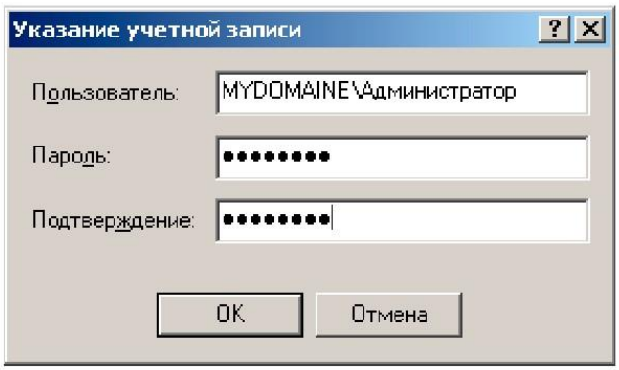
13. Создайте задания на выполнения архивации данных для папки *profiles,* используя выбор дополнительных возможностей:

- Выбираем тип архивирования (выберем «Обычный»).
- Ничего не меняем на странице «Способы архивации».
- На странице «Параметры архивации» можно выбрать замену существующих архивов или добавление архива (если файл с архивной копией уже существует).



14. На странице «Когда архивировать» задайте расписание для автоматического создания резервной копии — выберите вариант «Позднее» и задайте расписание архивирования, чтобы архивирование происходило по всем рабочим дням недели. Время начала установите, исходя из текущего времени системы + пять минут.

15. Нажмите далее. Система запросит имя и пароль пользователя, с чьими полномочиями будет выполняться задание архивирования. Рекомендуем для выполнения заданий резервного копирования создать специальные учетные записи, обладающие достаточными правами (как минимум члены группы «Операторы архива»).



16. Нажмем кнопку «Готово», задание будет создано, и оно появится в списке «Назначенных заданий». Теперь оно будет выполняться регулярно в соответствии с расписанием.

17. Завершите сеанс администратора, ожидайте до завершения задания. После проверьте результат.

Теневые копии.

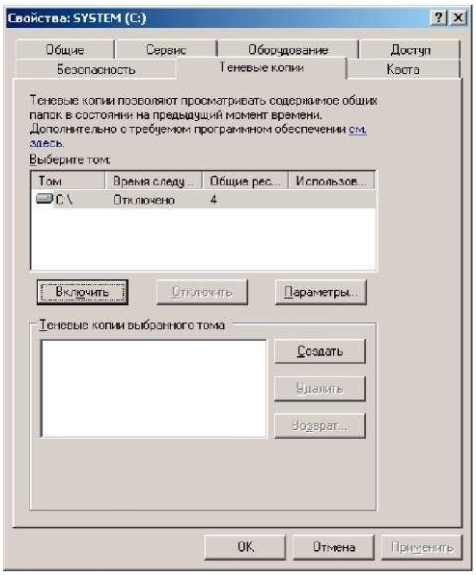
Эта технология, реализованная в Windows, позволяет архивировать открытые файлы с помощью создания «снимка» файловых ресурсов. По умолчанию теневые копии создаются на том же томе, где хранятся сетевые папки, поэтому они не смогут стать серьезной защитой от аппаратных аварий (например, выход из строя диска, на котором размещены эти данные). Можно настроить создание теневых копий на другом томе, что повысит уровень защиты. Теневые копии позволяют восстанавливать данные, ошибочно удаленные или модифицированные пользователями. При этом пользователи могут восстанавливать данные сами, без участия системного администратора. Теневые копии создаются только на томах с файловой системой NTFS.

Рассмотрим пример создания и использования теневых копий тома.

1. Создадим в сетевой папке на сервере файл *document.txt,* содержащий текст: «11111».

2. Откроем Свойства какого-либо тома и перейдем на закладку «Теневые копии». По умолчанию создание теневых копий для всех томов отключено.

3. Включим создание теневых копий для тома «С». При этом автоматически создастся первая теневая копия. В этом окне также можно вручную создать теневую копию данного тома в любой момент времени.



4. Настроим параметры теневого копирования. Для хранения теневых копий на томе требуется не менее 100 МБ дискового пространства, на каждом томе создается максимум 64 копии.

5. Настройте размер пространства для хранения копий в размере 200МБ и расписание создания теневых копий — дважды в день в 14-00 и 24-00.

6. На клиентской машине откройте файл document.txt и добавьте новую строку «22222».

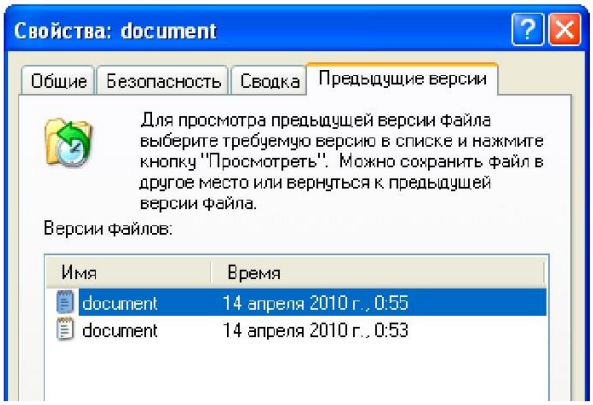
7. На сервере вручную создайте еще одну теневую копию данного тома.

8. На клиентской машине откройте файл *document.txt* и добавьте новую строку «33333».

Замечание. Теневые копии создаются не для всех файлов тома, а только для тех, которые размещены в папках, выставленных в сеть для общего доступа.

Использование теневых копий. После создания теневых копий пользователю становятся доступны Предыдущие версии файлов. Для использования этих возможностей нужна клиентская часть для доступа к теневым копиям. В системе Windows клиентская часть уже имеется в системе,

а для Windows ее нужно установить. Дистрибутив клиента теневых копий хранится на сервере в папке «%SystemRoot%\system32\clients\twcHent», в файле twcli32.msi. При установленном клиенте в свойствах файла, открываемого из сетевых папок, становится доступна закладка «Предыдущие версии». Проверьте, доступна ли данная закладка в Вашей клиентской системе, если нет, то установите необходимое ПО.



Пользователь теперь может просмотреть предыдущие копии, скопировать их в другой файл или восстановить содержимое файла в одно из предыдущих состояний. Закладка «Предыдущие версии» доступна в Свойствах не только конкретного файла, но и всей сетевой папки. Поэтому можно восстановить не только измененные файлы, но и ошибочно удаленные.

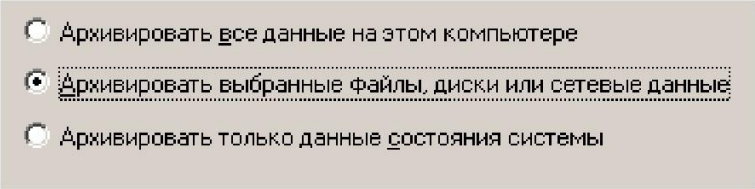
Архивирование и восстановление состояния системы.

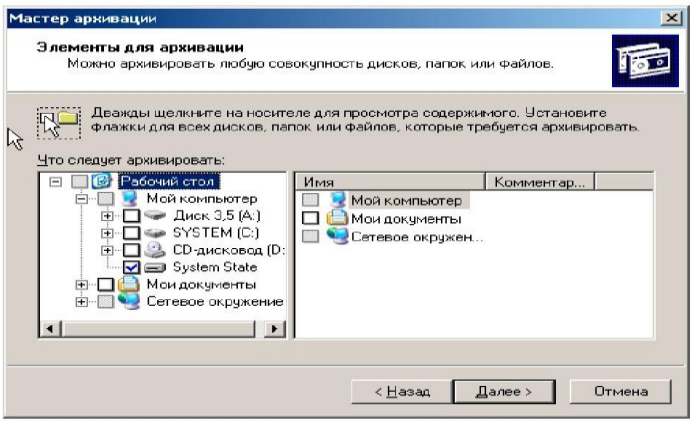
Большую часть работ по резервному копированию составляют задания на копирование бизнес-информации. Но имеется также возможность создания резервных копий для восстановления функционирования самой операционной системы. Есть два варианта архивирования системных данных — архивирование состояния системы (*System State)* и создания набора для

автоматического восстановления системы после аварии *(Automated System Recovery).*

Архивирование и восстановление состояния системы.

Для создания резервной копии состояния системы необходимо в утилите резервного копирования *ntbackup* при создании задания на архивирования отметить галочкой пункт *System State:*





При этом будут архивироваться следующие данные:

- системный реестр;
- база данных зарегистрированных классов объектов (*Class Registration);*
- системные загрузочные файлы;
- база данных служб сертификатов (только на серверах, на которых установлена служба сертификатов);

- база данных *Active Directory* и папка *SYSVOL* (на контроллерах доменов).

Для архивирования состояния системы, а также для последующего восстановления, обязательно нужны права администратора данного компьютера. Восстановление *Active Directory* необходимо выполнять только при загрузке системы в режиме восстановления служб каталогов (запуск меню выбора режимы загрузки операционной системы выбираются в начальный момент загрузки нажатием клавиши F8).

Автоматическое аварийное восстановление системы.

В отличие от резервного копирования состояния системы, при котором сохраняется только часть файлов операционной системы, резервное копирования для автоматического аварийного восстановления системы *(ASR, Automated System Recover)* архивирует больший объем информации практически весь том, на котором установлена операционная система. И процедура восстановления системы становится более сложной.

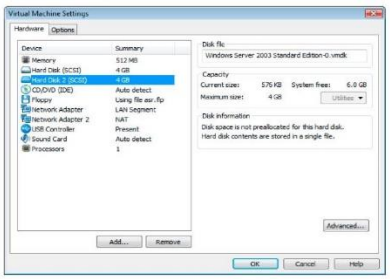
Создание ASR-копии.

На данном этапе потребуется носитель для создания резервной копии системного тома (порядка нескольких гигабайт), причем в случае восстановления системы этот носитель должен быть доступен мастеру установки операционной системы (т.е. это либо ленточный накопитель с драйверами для контроллера и накопителя, либо дисковый накопитель с соответствующими драйверами), а также чистая отформатированная дискета для сохранения информации о конфигурации резервной копии.

1. Выберем вариант хранения данных на дополнительном дисковом накопителе. Для этого выполним следующие действия:

- Завершим работу нашего сервера;

- В настройках данной ОС добавим новый SCSI-винчестер объемом 4Gb;



- Запустим ОС.

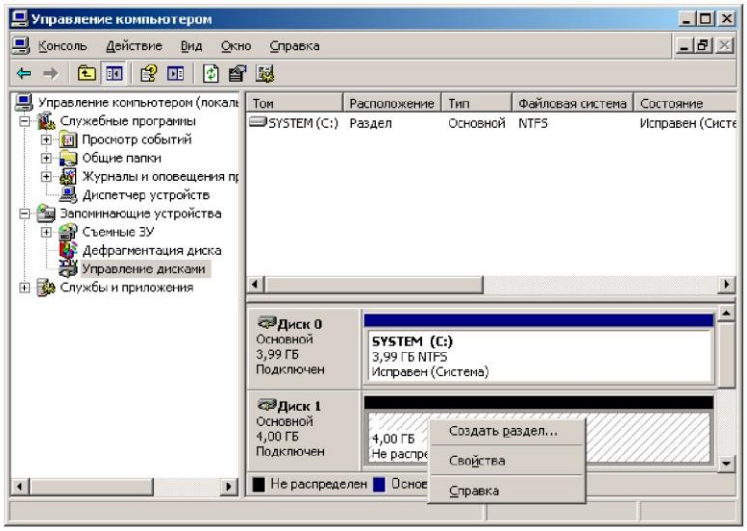
- Нажмем правой клавишей мыши на «Мой компьютер» и вызываем «Управление»;

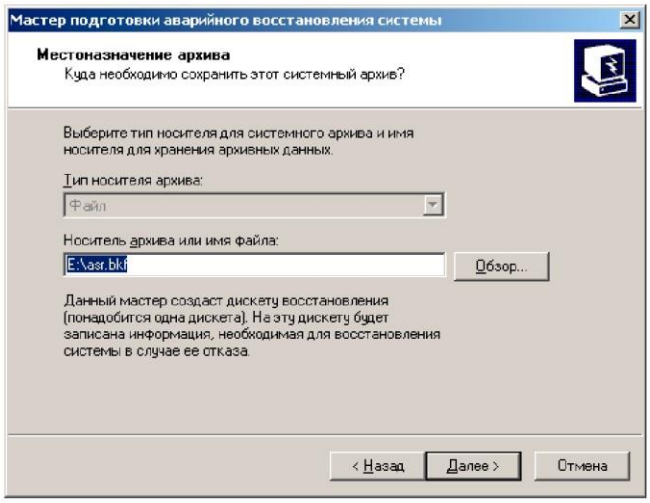
- В управлении дисками инициализируем новый диск; Создаем на нем основной NTFS раздел по всему объёму диска

2. Запустим утилиту резервного копирования ntbackup.

3. Запустим «Мастер аварийного восстановления системы».

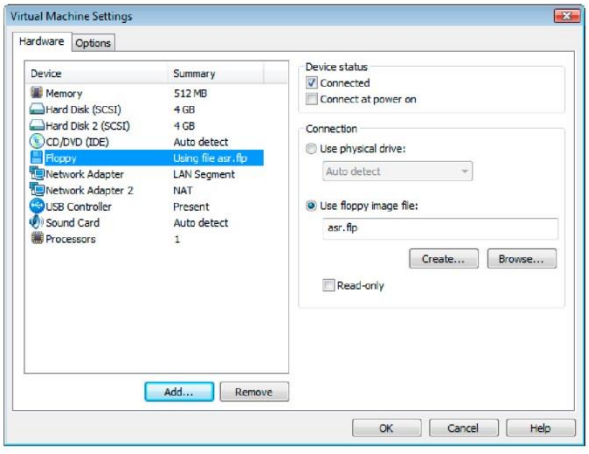
4. Укажем путь для сохранения архива.

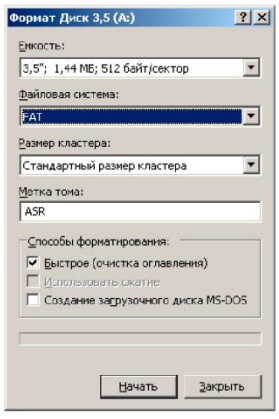




5. Нажмем кнопку «Готово». Утилита резервного копирования начнет создание резервной ASR-копии, в нужный момент будет сделан запрос вставить чистую дискету.

Работа с дисководом в WMware имеет определенную специфику. Будем использовать виртуальную дискету. Для этого в свойствах ОС сервера в WMware выберем дискету, выберем «Использовать образ дискеты» и нажмем «Создать». Перед использованием дискеты отформатируйте ее.





После записи конфигурации резервной копии утилита попросит пометить дискету соответствующей информацией (название резервной копии и дата создания).

Восстановление системы с помощью ASR-копии.

1. Подготовим все необходимое для аварийного восстановления системы: установочный CD с дистрибутивом операционной системы, носитель с резервной копией, дискету с конфигурацией ASR-копии.

2. Запустим процесс установки операционной системы с загрузочного компакт-диска для этого в BIOSe виртуальной машины сервера установим загрузку с CD;

3. На первой странице мастера установки системы (после появления синего экрана) нажать клавишу F2 для запуска процесса аварийного восстановления.

4. Далее мастер установки системы выполнит новую установку системы с форматированием системного тома.

5. После выполнения установки операционной системы автоматически запустится утилита резервного копирования, и система попросит вас указать путь к резервной копии для аварийного восстановления и вставить дискету с конфигурацией ASR-копии. Будет выполнено восстановление системы из аварийной резервной копии.

6. После завершения процесса восстановления будет воссоздан работоспособный сервер в той конфигурации, которая была до аварии (при условии, конечно, что, кроме самой системы, будут также восстановлены и данные, необходимые для работы сервера).

7. В BIOSe виртуальной машины сервера установим загрузку с HDD.

Корпорация Microsoft рекомендует использовать данный метод восстановления для серверов, выполняющих особые функции, которые трудно восстановить простой переустановкой и восстановлением данных. Если сервер не исполняет какие-либо особые роли, то Microsoft рекомендует на таких серверах архивировать только данные, а в случае аварии заново переустановить сервер, снова включить его в домен и восстановить данные из резервных копий.

Вывод. Сетевой администратор (ИТ-руководство компании) должны уделять вопросам резервного копирования самое пристальное внимание, т.к. от грамотно построенной и надежно работающей системы резервного копирования зависит, насколько быстро и удачно будет произведено восстановление информации, поврежденной в результате действий персонала, аппаратных сбоев, вирусных атак и прочих инцидентов.

Контрольные вопросы:

1. Какие причины резервирования данных?
2. Какие существуют типы резервного копирования?
3. Какие преимущества дает механизм теневых копий?
4. Какие типы резервного копирования Вы знаете? В чем их особенности?
5. Кто планирует какие данные нужно резервировать?
6. Какие недостатки имеет архивирование, проделанное в данной лабораторной работе?
7. Какие данные необходимо резервировать?

Список литературы

Основная литература:

1. Кучинский В.Ф. Сетевые технологии обработки информации [Электронный ресурс] : учебное пособие / В.Ф. Кучинский. – Электрон. текстовые данные. – СПб. : Университет ИТМО, 2015. – 118 с. – 2227-8397. – Режим доступа: http://www.iprbookshop.ru/68119.html

2. Оливер Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер. – Электрон. текстовые

данные. – Саратов: Профобразование, 2017. – 333 с – 978-5-4488-0054-2. – Режим доступа: http://www.iprbookshop.ru/63577.html

Дополнительная литература:

1. Архитектуры и топологии многопроцессорных вычислительных систем [Электронный ресурс] / А.В. Богданов [и др.]. – Электрон. текстовые данные. – М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 135 с. – 5-9556-0018-3. – Режим доступа: http://www.iprbookshop.ru/52189.html

2. Чекмарев Ю.В. Локальные вычислительные сети [Электронный ресурс] : учебное пособие / Ю.В. Чекмарев. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 200 с. – 978-5-4488-0111-2. – Режим доступа: http://www.iprbookshop.ru/63945.html

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к самостоятельной работе студентов по дисциплине Анализ и проектирование инфокоммуникационных сетей

для направления 09.04.02 «Информационные системы и технологии
профиль «Управление данными»
(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Оглавление

Введение

Дисциплина «Анализ и проектирование инфокоммуникационнных сетей» включена в программу подготовки магистров по направлению 09.04.02 – «Информационные системы и технологии» и относится к вариативной части профессионального цикла.

В рамках данной дисциплины предлагается изучение основ функционирования ЛВС и механизмов резервного копирования данных на базе операционной системы Windows Server. Для закрепления изученного материала предполагается выполнение лабораторных работ с использованием системы Windows Server Standard Edition. Трудоемкость дисциплины составляет 81 час.

Целью данной дисциплины «Анализ и проектирование инфокоммуникационных сетей» является формирование набора общенаучных и профессиональных компетенций будущего магистра по направлению подготовки 09.04.02 «Информационные системы и технологии»: выработка способности самостоятельно выполнять планирование, проектирование и разработку инфокоммуникационных сетей на основе различных технологий.

Задачи изучения дисциплины:

Изучение функционирования ЛВС на базе операционной системы Windows Server, а также механизмы резервного копирования данных в операционной системе Windows Server.

Для закрепления изученного материала предполагается выполнение лабораторных работ с использованием системы Windows Server Standard. Данная дисциплина призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов, изучению теоретических, методологических и практических проблем формирования, функционирования и развития информационных систем.

1. Организационно-методические рекомендации по освоению дисциплины

Самостоятельная работа студентов является важнейшим условием формирования научного способа познания. Она проводится накануне каждого практического и лабораторного занятия и включает выполнение конкретного практического задания.

Подготовленный материал, практическое задание оформляются в конспекте.

Самостоятельные занятия (СЗ) являются одной из активных форм обучения.

Самостоятельные занятия по дисциплине «Анализ и проектирование инфокоммуникационнных сетей» имеют целью:

- закрепить и углубить знания, полученные студентами на лекциях, на практических занятиях и в процессе лабораторных работ;

Самостоятельные занятия проводятся в специализированных аудиториях, оборудованных СВТ и возможностью пользования Интерентресурсом, в библиотеке.

Предлагаемые методические рекомендации содержат информацию для студентов, необходимую при подготовке и проведении лабораторных занятий по дисциплине«Анализ и проектирование инфокоммуникационнных сетей», а также могут быть полезны должностным лицам, в обязанности которых входит работа с организационно - распорядительными документами (ОРД).

ГОСТ Р 51141-08 определяет ОРД, как вид письменного документа, в котором фиксируют решение административных и организационных вопросов, а также вопросов управления, взаимодействия, обеспечения и регулирования деятельности органов власти, учреждений, предприятий, организаций, их подразделений и должностных лиц.

Согласно общероссийскому классификатору управленческой документации (ОКУД) ОРД классифицированы на четыре группы:

- организационно-правовая документация (уставы, положения, правила, штатное расписания, инструкции);
- распорядительная документация (приказы, распоряжения,

постановления, решения, указания);

- информационно - справочная документация (письма, телеграммы, факсы, акты, протоколы, докладные и служебные записки и др.); - документы по личному составу (заявления, личные карточки, приказы по личному составу и др.).

Оформление ОРД осуществляется в соответствии с требованиями ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».

Настоящий стандарт устанавливает: состав реквизитов документов; требования к оформлению реквизитов документов; требования к бланкам документов.

3. Методические указания по выполнению самостоятельной работы студентов

Методические указания должны включать следующие разделы:

– цель работы;

– задание, которое должно быть выполнено студентом в результате проведения самостоятельной работы;

– варианты индивидуальных заданий;

– основные теоретические положения, необходимые для выполнения задания, они должны быть краткими и содержать ссылки на литературу, в которой эти положения изложены в объеме, достаточном для выполнения самостоятельной работы;

– этапы выполнения задания с указанием конкретных сроков выполнения каждого из этапов и всего задания в целом;

– требования к оформлению графической и текстовой части самостоятельной работы;

– пример выполнения одного из вариантов задания и оформления отчета;

– библиографический список использованных источников.

4 Содержание самостоятельной работы

Название раздела (темы)	Цель определяется, исходя из компетентностного подхода	Форма контроля СРС	Задание для СРС	Требования к представлению и оформлению результатов СРС	Рекомендуемая литература
Технология Ethernet, Fast Ethernet.	Изучить технологию передачи информации для технологий Ethernet и Fast Ethernet в манчестерском коде.	Индивидуальное собеседование	Сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.	Письменно ответить на вопросы для контроля владения компетенциями данного практического занятия	**Основная литература:** 1. Кучинский В.Ф. Сетевые технологии обработки информации [Электронный ресурс] : учебное пособие / В.Ф. Кучинский. – Электрон. текстовые данные. – СПб. : Университет ИТМО, 2015. – 118 с. – 2227-8397. – Режим доступа: http://www.iprbookshop.ru/68119.html

Типы сетевых устройств.	Изучить основные типы сетевых устройств: сетевые карты, повторители, концентраторы, коммутаторы, маршрутизаторы, мосты.	Индивидуальное собеседование	Сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.	Письменно ответить на вопросы для контроля владения компетенциями данного практического занятия	2. Оливер Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 333 с – 978-5-4488-0054-2. – Режим доступа: http://www.iprbookshop.ru/63577.html **Дополнительная литература:** 1. Архитектуры и топологии многопроцессорных вычислительных систем [Электронный ресурс] / А.В. Богданов [и др.]. – Электрон. текстовые данные. – М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 135 с. – 5-9556-0018-3. – Режим доступа: http://www.iprbookshop.ru/52189.html 2. Чекмарев Ю.В. Локальные вычислительные сети [Электронный ресурс] : учебное пособие / Ю.В. Чекмарев. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 200 с. – 978-5-4488-0111-2. – Режим доступа: http://www.iprbookshop.ru/63945.html
Адресация в IPсетях.	Изучить автоматизацию процесса назначения	Индивидуальное собеседование	Сформулировать и письменно ответить на	Письменно ответить на вопросы	

	IP-адресов узлами сети протоколов DHCP.		вопросы для контроля владения компетенциями данного практического занятия.	для контроля владения компетенциями данного практического занятия	**Основная литература:** 1. Кучинский В.Ф. Сетевые технологии обработки информации [Электронный ресурс] : учебное пособие / В.Ф. Кучинский. – Электрон. текстовые данные. – СПб. : Университет ИТМО, 2015. – 118 с. – 2227-8397. – Режим доступа: http://www.iprbookshop.ru/68119.html 2. Оливер Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 333 с – 978-5-4488-0054-2. – Режим доступа: http://www.iprbookshop.ru/63577.html **Дополнительная литература:** 1. Архитектуры и топологии многопроцессорных вычислительных систем [Электронный ресурс] / А.В. Богданов [и др.]. – Электрон. текстовые данные. – М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 135 с. – 5-9556-0018-3. – Режим доступа: http://www.iprbookshop.ru/52189.html 2. Чекмарев Ю.В. Локальные вычислительные сети [Электронный ресурс] : учебное пособие / Ю.В. Чекмарев. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 200 с. – 978-5-4488-0111-2. – Режим доступа: http://www.iprbookshop.ru/63945.html
Алгоритмы маршрутизации.	Изучить основные требования, предъявляемые к алгоритму маршрутизации.	Индивидуальное собеседование	Сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.	Письменно ответить на вопросы для контроля владения компетенциями данного практического занятия	
Методы коммутации.	Изучить основные методы коммутации, достоинства и недостатки коммутации каналов.	Индивидуальное собеседование	Сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.	Письменно ответить на вопросы для контроля владения компетенциями данного практического занятия	

5. План-график выполнения самостоятельной работы студентов

№	Название контрольной точки	Срок ее сдачи
1.	Технология Ethernet, Fast Ethernet.	2
2.	Типы сетевых устройств	4
3.	Адресация в IP-сетях.	5
4.	Алгоритмы маршрутизации.	6
5.	Методы коммутации.	7

6. Организация контроля знаний студентов

6.1 Формы контроля знаний студентов

Контроль и оценка знаний, умений и навыков студентов осуществляется на лабораторных занятиях, консультациях, при приеме экзамена. В ходе контроля знаний преподаватель оценивает понимание студентом содержания дисциплины «Анализ и проектирование инфокоммуникационнных сетей», его способность применять методы управления при решении конкретных задач.

Контроль знаний студентов может осуществляться в следующих формах:

– текущий контроль знаний;

– итоговый контроль знаний.

Текущий контроль знаний студентов имеет целью:

– дать оценку работы каждого студента по усвоению им учебного материала, выявить недостатки в его подготовке и оказать практическую помощь в их устранении;

Основными формами текущего контроля знаний студентов являются:

- устный контрольный опрос;
- письменный контрольный блиц-опрос;
- защита лабораторной работы;
- защита практического занятия;
- промежуточное тестирование; - проверка конспектов лекций.

Устный контрольный опрос студентов проводится на лекциях (и лабораторных занятиях). По его результатам преподаватель оценивает качество подготовки студента к занятию.

Письменный контрольный блиц-опрос студентов проводится в течение запланированного преподавателем времени на лекциях и лабораторных занятиях путем письменного ответа их на поставленные вопросы, заданные преподавателем. Результаты его проведения отмечаются в журнале. На лабораторных занятиях знания и практические навыки студентов оцениваются по 4-балльной системе. Полученные оценки выставляется в журнале.

При проверке конспектов лекций дается анализ качества их ведения. Отмечаются допущенные ошибки, в рецензии преподавателя оценивается качество конспектирования учебного материала, даются рекомендации по улучшению качества конспектирования лекционного материала.

7. Рекомендации по работе с литературой и источниками

7.1. Рекомендации студентам по работе с литературой и источниками

Изучение литературы и источников необходимо начинать с прочтения соответствующих глав учебных изданий, учебных пособий или литературы, рекомендованной в качестве основной или дополнительной по дисциплине «Анализ и проектирование инфокоммуникационнных сетей» которые прямо или косвенно относятся к отрабатываемой теме.

Изучая литературу и источники, студенту рекомендуется вести краткий конспект. Однако не следует переписывать все содержание изучаемой темы, нужно выписывать лишь основные идеи и главные на ваш взгляд мысли. В отдельных случаях, когда встречаются важные определения, понятия, необходимый фактический материал и примеры, статистическая информация, имеющие отношение к изучаемой теме, студенту следует выписать их в виде цитат с полным указанием библиографических источников.

Конспектирование рекомендуемой литературы и источников необходимо вести с распределением собранных материалов по отдельным главам и параграфам согласно учебно-тематическому плану. Необходимо выписывать все выходные данные по используемой литературе и источникам.

Важным этапом при работе с рекомендуемой литературой и источниками является изучение законодательных и нормативных актов федерального, регионального, местного и ведомственного уровней. При изучении Указов Президента РФ, Законов и Кодексов РФ, постановлений, положений, рекомендаций и т.д., студент должен выяснить все изменения и дополнения, которые могли быть внесены после их выхода в свет.

Основой технологии интенсификации обучения на платформе цифровых образовательных технологий являются учебно-иллюстрационные материалы

(опорный конспект) по дисциплине «Анализ и проектирование инфокоммуникационнных сетей».

Работа с учебно-иллюстрационными материалами имеет следующие этапы:

1. Изучение теоретических основ учебного материала в аудитории: изложение преподавателем изучаемого материала студентам с объяснением по опорному конспекту;
2. Самостоятельная работа: индивидуальная работа студентов по опорному конспекту; фронтальное закрепление по блокам опорного конспекта.
3. Первое повторение - воспроизведение содержания заданной темы опорного конспекта по памяти.
4. Устное проговаривание материала опорного конспекта - необходимый этап внешнеречевой деятельности при усвоении учебного материала.
5. Второе повторение - взаимоопрос и взаимопомощь студентов друг другу.

Применение учебно-иллюстрационных материалов позволяет обобщить сложный по содержанию материал, активизировать мыслительную деятельность студентов.

Необходимо помнить, что главное для студента в самостоятельной работе с рекомендуемой литературой и источниками - это формирование своего индивидуального стиля, который может стать основой в будущей профессиональной деятельности.

7.2.Перечень рекомендуемой литературы

Основная литература:

1. Кучинский В.Ф. Сетевые технологии обработки информации [Электронный ресурс] : учебное пособие / В.Ф. Кучинский. – Электрон. текстовые данные. – СПб. : Университет ИТМО, 2015. – 118 с. – 2227-8397. – Режим доступа: http://www.iprbookshop.ru/68119.html

2. Оливер Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 333 c – 978-5-4488-0054-2. – Режим доступа: http://www.iprbookshop.ru/63577.html

Дополнительная литература:

1. Архитектуры и топологии многопроцессорных вычислительных систем [Электронный ресурс] / А.В. Богданов [и др.]. – Электрон. текстовые данные. – М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 135 c. – 5-9556-0018-3. – Режим доступа: http://www.iprbookshop.ru/52189.html

2. Чекмарев Ю.В. Локальные вычислительные сети [Электронный ресурс] : учебное пособие / Ю.В. Чекмарев. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 200 c. – 978-5-4488-0111-2. – Режим доступа: http://www.iprbookshop.ru/63945.html

в) программное обеспечение и Интернет-ресурсы

1) http://www.exponenta.ra – образовательный математический сайт;

2) http://www.mtuit.ru – Национальный открытый университет «ИНТУИТ»;

3) http://www.wmdow.edu.ru - Единое окно доступа к образовательным ресурсам.

Материально-техническое обеспечение дисциплины (модули)

1. Лекционная аудитория должна быть оборудована мультимедиа проектором.
2. Компьютерный класс из расчета одна ПЭВМ на два человека.