ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.ДВ.11.02 АДМИНИСТРИРОВАНИЕ СЕТЕЙ

Направление подготовки (специальность) 27.03.04 Управление в технических системах

Профиль образовательной программы «Интеллектуальные системы обработки информации и управления**»**

Форма обучения *очная*

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1.1. Лекция № 1 (2 часа)

Тема: «Задачи и цели сетевого администрирования, понятие о сетевых протоколах и службах».

1.1.1. Вопросы лекции:

1. Задачи и цели сетевого администрирования.
2. Модели межсетевого взаимодействия (модель OSI, модель DARPA).

1.1.2. Краткое содержание вопросов:

1. Задачи и цели сетевого администрирования.

Корпоративная сеть — сложная система, состоящая из программных, аппаратных и коммуникационных средств, обеспечивающих эффективное распределение вычислительных ресурсов. Основу работы сети составляют *сетевые службы* (или сервисы).

Базовый набор сетевых служб корпоративной сети:

- службы сетевой инфраструктуры DNS, DHCP, WINS;
- службы файлов и печати;
- службы каталогов;
- службы обмена сообщениями;
- службы доступа к базам данных.

Сетевое *администрирование* — это планирование, установка, настройка, обслуживание корпоративной сети, обеспечение ее надежной, бесперебойной, высокопроизводительной и безопасной работы

Задачи сетевого администрирования:

- Планирование сети
- Установка и настройка сетевых узлов
- Установка и настройка сетевых протоколов
- Установка и настройка сетевых служб
- Поиск неисправностей
- Поиск узких мест сети и повышения эффективности работы сети
- Мониторинг сетевых узлов
- Мониторинг сетевого трафика
- Защита информации в сети

2. Модели межсетевого взаимодействия (модель OSI, модель DARPA)

Для формального описания взаимодействия сетевых узлов используются межсетевые взаимодействия. В настоящее время стандартными моделями являются две сетевые модели: семиуровневая модель *OSI*, разработанная организацией *ISO* (Международная Организация по Стандартам), и четырехуровневая модель *TCP/IP*, разработанная в рамках проекта *DARPA*.

1.2. Лекция № 2 (2 часа)

Тема: «Сетевые операционные системы (на примере операционных систем семейства Windows Server); установка и настройка системы».

1.2.1. Вопросы лекции:

1. Операционные системы семейства Windows Server как базовый инструмент для изучения курса «Сетевое администрирование».

2. Обзор редакций и функциональных возможностей системы WindowsServer 2000/2003

1.2.2. Краткое содержание вопросов:

1. Операционные системы семейства *Windows Server* являются очень хорошим инструментом для изучения курса "Сетевое *администрирование*". Данные системы содержат богатый набор сетевых служб для изучения и практического освоения (при этом не потребуется приобретение специализированного дорогостоящего сетевого оборудования, достаточно иметь стандартный компьютерный *класс*, удовлетворяющий минимальным требованиям для установки системы):

- служба каталогов;
- службы сетевой инфраструктуры (DNS, DHCP, WINS);
- служба файлов и печати;
- сервер приложений (веб, электронная почта);
- службы терминалов;
- служба удаленного доступа/сервер виртуальной частной сети (VPN);
- сервер потокового мультимедиа-вещания.

2. Системы семейства *Windows Server* выпускаются в нескольких редакциях, каждая из которых содержит специфический для данной редакции набор сетевых служб и предъявляет свои требования к аппаратной конфигурации сервера, на котором данная система будет работать.

Планирование приобретения и установки системы в корпоративной сети требует рассмотрения и анализа широкого круга вопросов:

- определение набора ролей, которые будет выполнять данный сервер;
- расчет предполагаемой нагрузки на сервер (количество пользователей, объем обрабатываемой и передаваемой по сети информации);
- определение типа и количества процессоров и объема оперативной памяти;
- планирование дисковой подсистемы.

Процесс установки системы на сервере также требует предварительного планирования. Необходимо учесть такие параметры:

- способ установки (ручная или автоматическая);
- размещение дистрибутива системы (загрузочный CD, жесткий диск сервера, сетевая папка);
- будет ли система единственной на данном сервере или планируется использовать мультизагрузку различных экземпляров систем, установленных на различных дисках или различных разделах дисков;
- установка на "чистом" сервере или модернизация установленной ранее системы.

1.3. Лекция № 3 (2 часа)

Тема: «Сетевые операционные системы (на примере операционных систем семейства Windows Server); установка и настройка системы».

1.3.1. Вопросы лекции:

1. Установка и настройка системы.

1.3.2. Краткое содержание вопросов:

1. Установка и настройка системы.

- Запуск мастера установки системы.
- Сбор информации о системе и анализ конфигурации.
- Текстовый этап установки системы.
- Графический этап установки системы.
- Первоначальные действия по настройке сервера после установки операционной системы.
- Замечания по автоматической установке операционной системы Windows Server.

1.4. Лекция № 4 (2 часа)

Тема: «Протокол TCP/IP, служба DNS».

1.4.1. Вопросы лекции:

1. Основы функционирования протокола TCP/IP (IP-адрес, маска подсети, основной шлюз; деление на подсети с помощью маски подсети; введение в IP-маршрутизацию; утилиты TCP/IP).

2. Служба DNS (домены, зоны; зоны прямого и обратного просмотра; основные и дополнительные зоны; рекурсивный и итеративный запросы на разрешение имен).

3. Диагностические утилиты TCP/IP и DNS.

1.4.2. Краткое содержание вопросов:

1. Основы функционирования протокола TCP/IP (IP-адрес, маска подсети, основной шлюз; деление на подсети с помощью маски подсети; введение в IP-маршрутизацию; утилиты TCP/IP).

В сетях TCP/IP принято различать адреса сетевых узлов трех уровней

- физический (или локальный) адрес узла (MAC-адрес сетевого адаптера или порта маршрутизатора); эти адреса назначаются производителями сетевого оборудования;
- IP-адрес узла (например, 192.168.0.1), данные адреса назначаются сетевыми администраторами или Интернет-провайдерами;
- символьное имя (например, www.microsoft.com); эти имена также назначаются сетевыми администраторами компаний или Интернет-провайдерами.

Компьютеры или другие сложные сетевые устройства, подсоединенные к нескольким физическим сетям, имеют несколько IP-адресов — по одному на каждый сетевой интерфейс. Схема адресации позволяет проводить единичную, широковещательную и групповую адресацию. Таким образом, выделяют 3 типа IP-адресов.

1. Unicast-адрес (единичная адресация конкретному узлу) — используется в коммуникациях "один-к-одному".

2. Broadcast-адрес (широковещательный адрес, относящийся ко всем адресам подсети) — используется в коммуникациях "один-ко-всем". В этих адресах поле идентификатора устройства заполнено единицами. IP-адресация допускает широковещательную передачу, но не гарантирует ее — эта возможность зависит от конкретной физической сети. Например, в сетях Ethernet широковещательная передача выполняется с той же эффективностью, что и обычная передача данных, но есть сети, которые вообще не поддерживают такой тип передачи или поддерживают весьма ограничено.

3. Multicast-адрес (групповой адрес для многоадресной отправки пакетов) — используется в коммуникациях "один-ко-многим". Поддержка групповой адресации используется во многих приложениях, например, приложениях интерактивных конференций. Для групповой передачи рабочие станции и маршрутизаторы используют протокол IGMP, который предоставляет информацию о принадлежности устройств определенным группам.

2. Служба DNS (домены, зоны; зоны прямого и обратного просмотра; основные и дополнительные зоны; рекурсивный и итеративный запросы на разрешение имен).

DNS - это иерархическая база данных, сопоставляющая имена сетевых узлов и их сетевых служб IP-адресам узлов. Содержимое этой базы, с одной стороны, распределено по большому количеству серверов службы DNS, а с другой стороны, является централизованно управляемым. В основе иерархической структуры базы данных DNS лежит доменное пространство имен (domain namespace), основной структурной единицей которого является домен, объединяющий сетевые узлы (хосты), а также поддомены. Процесс поиска в БД службы DNS имени некоего сетевого узла и сопоставления этому имени IP-адреса называется "разрешением имени узла в пространстве имен DNS".

Служба DNS состоит из трех основных компонент:

- Пространство имен DNS и соответствующие ресурсные записи (RR, resource record) - это сама распределенная база данных DNS;
- Серверы имен DNS - компьютеры, хранящие базу данных DNS и отвечающие на запросы DNS-клиентов;
- DNS-клиенты (DNS-clients, DNS-resolvers) -компьютеры, посылающие запросы серверам DNS для получения ресурсных записей.

Системы семейства Windows Server поддерживают следующие типы зон:

- Стандартная основная (standard primary) - главная копия стандартной зоны; только в данном экземпляре зоны допускается производить какие-либо изменения, которые затем реплицируются на серверы, хранящие дополнительные зоны;
- Стандартная дополнительная (standard secondary) - копия основной зоны, доступная в режиме "только-чтение", предназначена для повышения отказоустойчивости и распределения нагрузки между серверами, отвечающими за определенную зону; процесс репликации изменений в записях зон называется "передачей зоны" (zone transfer) (информация в стандартных зонах хранится в текстовых файлах, файлы создаются в папке "%system root%\system32\dns", имя файла, как правило, образуется из имени зоны с добавлением расширения файла ".dns"; термин "стандартная" используется только в системах семейства Windows);
- Интегрированная в Active Directory (Active Directory–integrated) - вся информация о зоне хранится в виде одной записи в базе данных Active Directory (такие

типы зон могут существовать только на серверах Windows, являющихся контроллерами доменов Active Directory; в интегрированных зонах можно более жестко управлять правами доступа к записям зоны; изменения в записях зоны между разными экземплярами интегрированной зоны производятся не по технологии передачи зоны службой DNS, а механизмами репликации службы Active Directory);

- Зона-заглушка (stub ; только в Windows 2003) - особый тип зоны, которая для данной части пространства имен DNS содержит самый минимальный набор ресурсных записей (начальная запись зоны SOA, список серверов имен, отвечающих за данную зону, и несколько записей типа A для ссылок на серверы имен для данной зоны).

3. Диагностические утилиты TCP/IP и DNS

Любая операционная система имеет набор диагностических утилит для тестирования сетевых настроек и функционирования коммуникаций. Большой набор диагностических средств есть и в системах семейства Windows (как графических, так и режиме командной строки).

1.5. Лекция № 5 (2 часа)

Тема: «Служба каталогов Active Directory».

1.5.1. Вопросы лекции:

1. Основные термины и понятия (лес, дерево, домен, организационное подразделение). Планирование пространства имён AD. Установка контроллеров доменов.

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

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

4. Система безопасности (протокол Kerberos, настройка параметров системы безопасности).

1.5.2. Краткое содержание вопросов:

1. Основные термины и понятия (лес, дерево, домен, организационное подразделение). Планирование пространства имён AD. Установка контроллеров доменов.

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

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

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

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

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

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

Контроллеры домена были подробно описаны в предыдущем разделе.

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

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

Всего имеется пять специализированных ролей:

- Schema Master (хозяин схемы)
- Domain Naming Master (хозяин именования доменов)
- PDC Emulator (эмулятор PDC)
- RID Master (хозяин RID, распределитель идентификаторов учетных записей)
- Infrastructure Master (хозяин инфраструктуры)

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

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

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

- Локальные учетные записи пользователей.
- Учетные записи пользователей домена.
- Встроенные учетные записи.

4. Система безопасности (протокол Kerberos, настройка параметров системы безопасности).

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

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

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

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

1.6. Лекция № 6 (2 часа)

Тема: «Служба файлов и печати (на примере Windows Server)».

1.6.1. Вопросы лекции:

1. Базовые и динамические диски, тома. Файловые системы FAT16, FAT32, NTFS.
2. Права доступа, наследование прав доступа, взятие во владение, аудит доступа к ресурсам.
3. Сжатие и шифрование информации. Квоты. Дефрагментация.

1.6.2. Краткое содержание вопросов:

1. Базовые и динамические диски, тома. Файловые системы FAT16, FAT32, NTFS.

Базовые, или основные, диски — это термин, обозначающий дисковые конфигурации, использовавшиеся в системах корпорации Microsoft до появления Windows 2000. После выхода Windows данные технологии приобрели название "базовый (основной)" диск (basic disk) для того, чтобы отличить их от новых технологий управления дисками, которые стали называть " динамическими " (dynamic disks).

В системах с DOS-ядром (MS DOS, Windows 3/95/98/ME) базовый диск мог состоять из одного или двух разделов. Если разделов два, то первый называется " основным " разделом (primary partition), а второй — " дополнительным " (secondary partition). Дополнительный раздел в свою очередь может быть разбит на несколько логических дисков (logical disks). В системах с ядром Windows NT (Windows NT/2000/XP/2003) на жестком диске может быть до четырех разделов. При этом все разделы могут быть основными либо один из них — дополнительный (который можно опять же разбить на логические диски).

Каждому основному разделу или логическому диску в системе может быть назначена буква диска (C:, D: и т.д.). В системе Windows 2003, если нет флоппи-дисков, то буквы для разделов и логических дисков можно назначать, начиная с A:.

2. Права доступа, наследование прав доступа, взятие во владение, аудит доступа к ресурсам.

Определение прав доступа к файловым ресурсам осуществляется на основе разрешений (permissions). При определении разрешений к ресурсам, предоставленным в совместный доступ в сети, используются два типа разрешений: сетевые разрешения (shared folder permissions) и разрешения, заданные в файловой системе NTFS (NTFS-permissions).

Рассмотрим сначала сетевые разрешения. Данный вид разрешений не зависит от типа файловой системы. Сетевые разрешения применяются только при доступе к ресурсам через сеть. Если пользователь локально вошел в систему (локально зарегистрировался в системе), то, какие бы ни были назначены сетевые разрешения для определенной папки, эти разрешения не будут применяться ни к самой папке, ни к размещенным в ней файлам. В случае локальной регистрации пользователя, если данные размещены на томе с системой FAT, пользователь имеет полный доступ к этим данным, если данные размещены на томе NTFS, права доступа будут определяться разрешениями NTFS.

3. Сжатие и шифрование информации. Квоты. Дефрагментация.

Для экономии дискового пространства можно какие-либо папки или файлы сделать сжатыми. Процесс сжатия выполняется драйвером файловой системы NTFS. При открытии файла в программе файловая система распаковывает файл, после внесения изменений в файл при сохранении на диск файл снова сжимается. Делается это совершенно прозрачно для пользователя и не доставляет пользователю никаких хлопот.

Системы семейства Windows 2000/XP/2003 и более поздние позволяют шифровать данные, хранящиеся на томе с системой NTFS. Шифрование данные осуществляется так же легко, как и их сжатие. Шифрование является надежным средством предотвращения несанкционированного доступа к информации, даже если будет похищен компьютер с этой информацией или жесткий диск из компьютера. Если данные зашифрованы, то доступ к ним имеет (с небольшим исключением) только тот пользователь, который выполнил шифрование, независимо от установленных разрешений NTFS. Шифрование производится компонентой " Шифрованная файловая система " (EFS, Encrypted File System), являющейся составной частью файловой системой NTFS.

1.7. Лекция № 7 (2 часа)

Тема: «Сетевые протоколы и службы».

1.7.1. Вопросы лекции:

1. Обзор сетевых протоколов NetBEUI, IPX/SPX, DLC; служб DHCP, WINS, RRAS.

2. Термины и понятия сетевой печати. Установка драйверов, настройка принтеров. Протокол IPP (Internet Printing Protocol).

1.7.2. Краткое содержание вопросов:

1. Обзор сетевых протоколов NetBEUI, IPX/SPX, DLC; служб DHCP, WINS, RRAS.

Протокол NetBEUI (NetBIOS Extended User Interface) ведет свою историю от сетевого программного интерфейса NetBIOS (Network Basic Input/Output System),

появившегося в 1984 году как сетевое расширение стандартных функций базовой системы ввода/вывода (BIOS) IBM PC для сетевой программы PC Network фирмы IBM.

Служба DHCP (Dynamic Host Configuration Protocol) — это одна из служб поддержки протокола TCP/IP, разработанная для упрощения администрирования IP-сети за счет использования специально настроенного сервера для централизованного управления IP-адресами и другими параметрами протокола TCP/IP, необходимыми сетевым узлам.

Служба WINS (Windows Internet Name Service) выполняет задачи, аналогичные задачам службы DNS, — динамическая регистрация имен компьютеров и других сетевых узлов и их IP-адресов в БД сервера WINS и разрешение имен компьютеров в IP-адреса. Главное отличие в том, что WINS функционирует в совершенно ином пространстве имен, т.н. пространстве имен NetBIOS, которое никак не пересекается с пространством FQDN-имен, в котором работает служба DNS. По этой причине службу WINS еще иначе называютNetBIOS Name Service (NBNS).

2. Термины и понятия сетевой печати. Установка драйверов, настройка принтеров. Протокол IPP (Internet Printing Protocol).

Основные термины, используемые в данном пункте.

- Устройство печати (Print device) — физическое устройство, на котором осуществляется вывод информации на бумагу или иные виды носителей;
- Принтер (Printer) — объект операционной системы (программный интерфейс между системой и портом);
- Порт (Port) — объект системы, связывающий принтер и устройство печати;
- Драйвер принтера (Printer driver) — программная компонента, преобразующая информацию из компьютера в набор команд, соответствующий данной модели устройства печати;
- Сервер печати (Print server) — компьютер, получающий от приложений, работающих на компьютерах в сети, задания на печать документов;
- Очередь печати (Print queue) — очередь документов, ожидающих вывода на устройство печати;
- Спулер (Spooler) — компонента системы, которая временно сохраняет на жестком диске сервера документы, содержащиеся вочереди печати.

1.8. Лекция № 8 (2 часа)

Тема: «Служба резервного копирования».

1.8.1. Вопросы лекции:

1. Архивирование и восстановление файловых ресурсов.
2. Архивирование и восстановление состояния системы.

1.8.2. Краткое содержание вопросов:

1. Архивирование и восстановление файловых ресурсов.

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 увсех заархивированных файлов очищается атрибут " Файл готов для архивирования ".

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.

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.

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.

2. 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).

1.9. Лекция № 9 (2 часа)

Тема: «Службы терминалов».

1.9.1. Вопросы лекции:

1. Режим удалённого управления. Режим сервера приложений, лицензирование использования служб терминалов.

2. Мониторинг сетевых устройств. Мониторинг серверов (просмотр событий, аудит, мониторинг производительности, определение узких мест).

1.9.2. Краткое содержание вопросов:

1. Режим удалённого управления. Режим сервера приложений, лицензирование использования служб терминалов.

В режиме удаленного управления к терминальным службам могут подключаться только пользователи, обладающие административными привилегиями (в Windows 2003 — также пользователи, включенные в группу " Пользователи удаленного рабочего стола "). Сервер будет сконфигурирован для выполнения не более двух клиентских сеансов управления (при этом не требуются клиентские лицензии). В данном режиме к минимуму сведено снижение производительности сервера, неизбежное при запуске служб терминалов (приложения, которые запускает пользователь в сеансе удаленного рабочего стола на сервере работают с низким приоритетом, более высокие приоритеты распределяются системным службам). Поэтому специалисты корпорации Microsoft

рекомендуют устанавливать терминальные службы в режиме удаленного управления на всех серверах Windows.

2. Мониторинг сетевых устройств. Мониторинг серверов (просмотр событий, аудит, мониторинг производительности, определение узких мест).

Мониторинг сетевых устройств — это постоянное наблюдение за деятельностью данных устройств, поиск проблем и неисправностей в их работе, принятие решений о ликвидации проблем и неисправностей, повышению эффективности функционирования устройств.

Консоль " Просмотр событий " позволяет просматривать события, регистрируемые системой и относящиеся к функционированию различных системных компонент:

- самой операционной системы (журнал " Система ");
- подсистемы безопасности (журнал " Безопасность ");
- подсистемы исполнения приложений (журнал " Приложения ");
- службы каталогов (для контроллеров доменов, журнал " Служба каталогов ");
- службы DNS (если на сервере установлена служба DNS, журнал " DNS-сервер ");
- службы репликации файлов (для контроллеров доменов, журнал " Служба репликации файлов ").

Задача сетевого администратора — регулярный просмотр системных журналов с целью своевременного обнаружения уже возникших или предупреждения потенциальных неисправностей или атак злоумышленников. Для более удобного просмотра событий можно создать отдельную консоль, в которой будут отображаться события группы серверов и, возможно, отдельных рабочих станций.

Аудит различных событий заключается в разработке и реализации в системе политик аудита. Набор категорий событий, подлежащих аудиту, необходимо формировать на основе требований безопасности компании/организации и потенциальных угроз системе безопасности.

После определения и настройки политик аудита задача администратора снова сводится к регулярному просмотру журналов событий (в первую очередь — журнала "Безопасность").

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ (СЕМИНАРСКИХ) ЗАНЯТИЙ

2.1. Практическое (семинарское) занятие №1 (2 часа).

Тема: «Знакомство с задачами сетевого администрирования. Создание моделей межсетевого взаимодействия».

2.1.1. Вопросы к занятию:

1. Цель компьютерной сети – предоставление доступа к её ресурсам.
2. Различие между понятиями сетевого и системного администрирования
3. Задачи сетевого администрирования
4. Модель OSI (Open System Interconnection – взаимодействие открытых систем)
5. Модель TCP/IP
6. Сеть и технология Frame Relay
7. Сеть и технология ATM

2.1.2. Краткое описание проводимого занятия:

2.1.2.1. Ответы на вопросы семинарского (практического) занятия.

2.1.2.2. Проведение текущего контроля успеваемости

Задания для проведения текущего контроля успеваемости

1) История развития сети Internet
2) Основные инструменты Internet
3) Адресация в Интернете. IP-адрес
4) Стек протоколов TCP/IP

2.1.2.3. Выборочная проверка самостоятельного изучения вопросов:

1. Задачи и цели сетевого администрирования, понятие о сетевых протоколах и службах.

2.1.2.4. Выборочная проверка ИДЗ-1: установка операционных систем семейства Windows 2003 Server.

2.2. Практическое (семинарское) занятие № 2 (2 часа).

Тема: «Установка и настройка системы».

2.2.1. Вопросы к занятию:

1. Консоль управления (Microsoft Management Console, MMC);
2. Мастера (Wizards);
3. Утилиты командной строки.

2.2.2. Краткое описание проводимого занятия:

2.2.2.1. Ответы на вопросы семинарского (практического) занятия.

2.2.2.2. Проведение текущего контроля успеваемости

Задания для проведения текущего контроля успеваемости

1) Система доменных имен. Принципы организации
2) Система доменных имен. Регистрация

2.2.2.3. Выборочная проверка самостоятельного изучения вопросов:

1. Сетевые операционные системы. Установка и настройка системы

2.2.2.4. Выборочная проверка ИДЗ-3: работа с программой ping.exe.

2.3. Практическое (семинарское) занятие № 3 (2 часа).

Тема: «Изучение функционирования протокола TCP/IP».

2.3.1. Вопросы к занятию:

1. IP-адрес, маска подсети, основной шлюз;
2. Деление на подсети с помощью маски подсети.

2.3.2. Краткое описание проводимого занятия:

2.3.2.1. Ответы на вопросы семинарского (практического) занятия.

2.3.2.2. Проведение текущего контроля успеваемости

Задания для проведения текущего контроля успеваемости

1) Электронная почта в Internet. Протокол POP
2) Формат представления почтовых сообщений MIME

2.3.2.3. Выборочная проверка самостоятельного изучения вопросов:

1. Служба каталогов Active Directory

2.3.2.4. Выборочная проверка ИДЗ-5: Диагностические утилиты для протокола TCP/IP.

2.4. Практическое (семинарское) занятие № 4 (2 часа).

Тема: «Планирование пространства имен AD. Управление пользователями и группами».

2.4.1. Вопросы к занятию:

1. Установка контроллеров доменов.
2. Управление организационными подразделениями, делегирование полномочий.
3. Групповые политики.

2.4.2. Краткое описание проводимого занятия:

2.4.2.1. Ответы на вопросы семинарского (практического) занятия.

2.4.2.2. Проведение текущего контроля успеваемости

Задания для проведения текущего контроля успеваемости

1)Каковы функции клиентской и серверной частей сетевой службы?

2)Как связаны сетевая служба и сетевой порт?

3)Назовите два протокола динамического обнаружения сетевых служб, которые поддерживаются в Lion.

4) Как Lion использует протоколы динамического обнаружения сетевых служб для доступа к ним?

2.4.2.3. Выборочная проверка самостоятельного изучения вопросов:

1. Служба файлов и печати.

2.4.2.4. Выборочная проверка ИДЗ-7: процесс установки контроллера домена.

2.5. Практическое (семинарское) занятие № 9 (2 часа).

Тема: «Служба DNS. Система безопасности».

2.5.1. Вопросы к занятию:

1. Домены, зоны; зоны прямого и обратного просмотра
2. Основные и дополнительные зоны
3. Рекурсивный и итеративный запросы на разрешение имен.
4. Протокол Kerberos
5. Настройка параметров системы безопасности.

2.5.2. Краткое описание проводимого занятия:

2.5.2.1. Ответы на вопросы семинарского (практического) занятия.

2.5.2.2. Проведение текущего контроля успеваемости

Задания для проведения текущего контроля успеваемости

1) Назовите пять сетевых файловых служб, с которыми можно соединиться из диалогового окна Подключение к серверу (Connect to Server) утилиты Finder.

2)Как заполняются объекты внутри папки Сеть (Network) утилиты Finder?

2.5.2.3. Выборочная проверка самостоятельного изучения вопросов:

1. Служба файлов и печати.

2.5.2.4. Выборочная проверка ИДЗ-9: способы управления групповыми политиками.

2.6. Практическое (семинарское) занятие № 15 (2 часа).

Тема: «Установка драйверов, настройка принтеров».

2.6.1. Вопросы к занятию:

1. Установка и настройка принтера, предоставление общего доступа к принтеру по сети;
2. Настройка сервера печати;
3. Подключение клиентского ПК к серверу печати, загрузка драйверов;
4. Перенаправление портов;

2.6.2. Краткое описание проводимого занятия:

2.6.2.1. Ответы на вопросы семинарского (практического) занятия.

2.6.2.2. Проведение текущего контроля успеваемости

Задания для проведения текущего контроля успеваемости

1) Какой протокол электронной почты работает принципу "stop-go"?

а) SMTP;

б) POP;

в) UUCP;

г) а и б;

2) Что входит в основу Telnet?:

а) концепция сетевого виртуального терминала (Network Virtual Terminal) или NVT;

б) принцип договорных опций (согласование параметров взаимодействия);

в) симметрия связи “терминал-процесс”;

г) все три компонента входят в основу Telnet.

3) Номер порта протокола Telnet?

а) 20;

б) 30;

в) 23;

г) 80

2.6.2.3. Выборочная проверка самостоятельного изучения вопросов:

1. Режим сервера приложений, лицензирование использования служб терминалов.

2.6.2.4. Выборочная проверка ИДЗ-15: управление сервером с помощью консоли MMC и создание собственных консолей.

2.7. Практическое (семинарское) занятие № 16 (2 часа).

Тема: «Протокол IPP (Internet Printing Protocol)».

2.7.1. Вопросы к занятию:

1. Управление печатью
2. Поддержка контроля доступа
3. Аутентификация и шифрование

2.7.2. Краткое описание проводимого занятия:

2.7.2.1. Ответы на вопросы семинарского (практического) занятия.

2.7.2.2. Проведение текущего контроля успеваемости

Задания для проведения текущего контроля успеваемости

1) Какой из принципов построения URL адресов в WWW лишний?

а) расширяемость;

б) полнота;
в) читаемость;
г) универсальность.

2) Какой из ниже перечисленных методов позволяет получить данные возвращаемые Web-сервером в форме URL?
а) GET;
б) POST;
в) HEAD.
г) а и б;

2.7.2.3. Выборочная проверка самостоятельного изучения вопросов:
1. Режим сервера приложений, лицензирование использования служб терминалов.
2.7.2.4. Выборочная проверка ИДЗ-16: работа с консолью "Удаленные рабочие столы".

2.8. Практическое (семинарское) занятие № 17 (2 часа).
Тема: «Служба резервного копирования».
2.8.1. Вопросы к занятию:
1. Полное резервное копирование (Full backup)
2. Дифференциальное резервное копирование (Differential backup)
3. Инкрементное резервное копирование (Incremental backup)
2.8.2. Краткое описание проводимого занятия:
2.8.2.1. Ответы на вопросы семинарского (практического) занятия.
2.8.2.2. Проведение текущего контроля успеваемости
Задания для проведения текущего контроля успеваемости
1) Какой порт использует протокол HTTP?
а) 20;
б) 80;
в) 21
г) 23.

2) Какой порт использует протокол SMTP?
а) 25;
б) 20;
в) 80;
г) 23;

3) Какой день считается днем рождения сети Интернет?
а) 8 марта 1958 года;
б) 23 февраля 1975 года;
в) 1 января 1983 года;
г) 7 ноября 1991 года

4) Какой протокол использует 110 порт стека TCP/IP?
а) HTTP;
б) POP3;
в) FTP;
г) SMTP

5) Основное назначение какого тега является создание однострочного текстового поля?

а) < INPUT TYPE=TEXT >;

б) < TEXTAREA >;

в) < INPUT TYPE= TEXTAREA >;

г) <OPTION> .

2.8.2.3. Выборочная проверка самостоятельного изучения вопросов:

1. Режим сервера приложений, лицензирование использования служб терминалов.

2.8.2.4. Выборочная проверка ИДЗ-17: запуск и настройка программы резервного копирования и восстановления данных и системы в Windows Server 2003.