Учреждение образования
«Белорусский государственный университет культуры и искусств»

Факультет культурологии и социально-культурной деятельности

Кафедра информационных технологий в культуре

СОГЛАСОВАНО
Заведующий кафедрой
_____П.В.Гляков
30.09.2017 г.

СОГЛАСОВАНО
Декан факультета
_____Н.Н.Королев
28.09.2017 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
АДМИНИСТРИРОВАНИЕ КОРПОРАТИВНЫХ СЕТЕЙ

Специальность 1-21 04 01 Культурология,
направление специальности 1-21 04 01-02 Культурология (прикладная),
специализация 1-21 04 01-02 04 Информационные системы в культуре

Составитель: А.Г.Зезюля, доцент кафедры информационных технологий в культуре

Рассмотрено и утверждено на заседании Совета университета
19 сентября 2017 г., протокол № 1

Составитель:

Зезюля А.Г., доцент кафедры информационных технологий в культуре Белорусского государственного университета культуры и искусств

Рецензенты:

Рассмотрен и рекомендован к утверждению:

Кафедрой информационных технологий в культуре
(протокол от 31.08.2017 г. № 1);

Советом факультета культурологии и СКД
(протокол от 30.08.2017 г. № 1)

Оглавление

1. ПОЯСНИТЕЛЬНАЯЗАПИСКА

Учебно-методический комплекс по дисциплине по выбору «Администрирование корпоративных сетей» представляет собой систему учебно-методических материалов, предназначенных для создания эффективной поддержки учебного процесса студентов.

Комплекс предназначен для достаточно глубокого теоретического и практического освоения студентами учебного материала, предусмотренного содержанием учебной программы по дисциплине.

Учебный материал систематизирован в удобной для усвоения форме и выполнен в соответствии с требованиями образовательного стандарта.

Важной особенностью комплекса является использование системного подхода к изучение теоретических основ компьютерных сетей и практического их использования в деятельности учреждений культуры и искусств.

Учебно-методические материалы, содержащиеся в комплексе, предусматривают достаточно глубокое и полное усвоение студентами знаний устройства и безопасного функционирования компьютерных сетей на уровне предприятия.

Цель учебно-методического комплекса полное, удобное и эффективное обеспечение учебного процесса по учебной дисциплине «Администрирование корпоративных сетей» для студентов культурологического профиля.

2. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

Лекция 1.ОСНОВНЫЕ ПОНЯТИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Эволюциярежимов работы компьютерных систем.

Для ЭВМ 1-го поколения характерен *монопольный* режим работы.

Этот режим характеризуется тем, что во время сеанса все вычислительные ресурсы принадлежат одному пользователю (задаче, приложению) монопольно.

Это позволяет реализовать диалоговый (интерактивный) режим взаимодействия с ЭВМ. Т.е. в процессе работы пользователь имеет возможность оперативно координировать свои действия с учетом результата взаимодействия на предыдущих шагах выполнения работы непосредственно во время сеанса.

Интерактивность монопольного режима обеспечивает достаточно эффективную поддержку функционирования автоматизированных информационных систем в реальном времени.

Важным недостатком монопольного режима является неэффективное использование вычислительных мощностей ЭВМ за счет рассогласования скорости ввода информации и скорости её обработки процессором. Как правило, в монопольном режиме наблюдаются значительные потери процессорного времени, т.е. процессор занят обработкой информации незначительную часть времени (по некоторым оценкам всего 2-3% от времени сеанса).

Монопольный режим был характерен для использования ЭВМ первого поколения. Ясно, что в условиях высокой стоимости машинного времени, этот режим являлся неэффективным.

Поэтому актуальной являлась задача разработки более эффективного режима работы, который в значительной степени позволил бы повысить коэффициент загрузки процессора.

С этой целью использовался *пакетный* режим обработки информации, который часто применялся при работе с машинами второго поколения. Производительность машин 2-го поколения, выполненых на дискретных полупроводниковых элементах (транзисторах, диодах, динисторах, тиристорах и т.п), возросла по сравнению с 1 поколением в среднем приблизительно в сто раз. Скорость выполнения транзакций ввода на основе ручного ввода практически не изменилась. Чтобы повысить коэффициент загрузки процессора применялся высокоскоростной ввод с помощью специальных высокоскоростных устройств считывания со специальных промежуточных носителей информации (перфокарт и перфолент). Подготовка этих промежуточных носителей происходила в центрах подготовки информации, которые были оснащены специальным оборудованием (перфораторами, контрольниками и проч.) и специально подготовленным персоналом. Перфораторщицы обеспечивали перенос информации с традиционных носителей на перфоленты и перфокарты, а затем правильность набора контролировалась при считывании и распечатке информации с помощью контрольников. При наличии ошибок, вносились исправления. Исправленный пакет перфокарт или перфоленты передавались непосредственно на ЭВМ. С

помощью высокоскоростных устройств ввода выполнялось считывание информации с указанных носителей, которая помещалась в оперативную память ЭВМ. Запускался вычислительный процесс и после обработки, полученные результаты выводились на печать.

Пакетный режим в значительной мере повысил коэффициент использования процессорного времени, но практически исключил оперативный интерактивный режим, т.е. практически было невозможно управлять вычислительным процессом в диалоговом режиме. Хотя пакетный режим в целом привел к более эффективному использованию машинного времени, но оперативность выполнения задач в целом с использованием пакетного режима была реально снижена.

Объединение преимуществ монопольного и пакетного режимов работы представляет многотерминальный режим работы с *разделением времени*. Этот режим, характерный для 3 поколения ЭВМ для которых элементной базой являлись интегральные микросхемы малой (до 10 активных элементов), средней (до 100) и большой (до 1000) степени интеграции, в первую очередь связан с отходом от классической фон неймановской структуры.

Согласно принципам фон Неймана обработка информации осуществляется в оперативной памяти ЭВМ с помощью арифметико-логического устройства (АЛУ) под управлением устройства управления (УУ). Традиционно рассматривалось одно устройство ввода информации в ЭВМ и устройство вывода для вывода результата.

Поскольку производительность процессора возросла еще в среднем около 100 крат по сравнению с машинами 2-го поколения, то скорость ввода информации должна была также значительно возрасти для сохранения коэффициента использования процессора.

Это было достигнуто подключением к ЭВМ (мэйнфрейму) многих рабочих станций (терминалов), каждая из которых представляла собой объединение устройств ввода и вывода (отображения) информации, снабженых буферной памятью.

Операторы терминалов вводили информацию в буферную память терминалов в автономном режиме. Центральная ЭВМ с помощью адаптера последовательно сканировала состояние терминалов и, в случае, готовности терминала выполняла считывание информации, решение задачи и вывод результата на соответствующий терминал. При высокой скорости обработки информации процессором у пользователей создавалась иллюзия *монопольного* владения вычислительными ресурсами, хотя реально обеспечивалась последовательная обработка задач. Описанный режим работы несколько упрощён. Обычно режим разделения времени использовал прерывания работы процессора через заданные промежутки времени и работу в многозадачном режиме, при котором разделение времени осуществлялось равномерно между задачами, а не терминалами. Развитие и совершенствование режима разделения времени позволило в значительной мере повысить не только эффективность работы однопроцессорных многопользовательских систем, но и явилась основой для разработки и создания компьютерных сетей.

С внедрением использования терминалов стала реализовываться служба удаленных терминалов, особенностью которой было обслуживание терминалов удаленных на сотни, а иногда тысячи километров от центральной ЭВМ. Практически одновременно необходимо было решить вопросы связи удаленных ЭВМ. Это положило основу становления и развития глобальных сетей 60-70 годах прошлого столетия.

Проблема взаимодействия нескольких компьютеров внутри относительно небольшого предприятия, для которых имелась возможность использовать организовать специализированную информационно-коммуникационную среду начала усиленно решаться при появлении мини-компьютеров и персональных ЭВМ в 70-80 годах XX века.

Сетевой режим работы основан на использовании информационно-коммуникационной среды многими участниками сетевого взаимодействия. Этот режим является основным режимом использования средств компьютерной техники четвертого поколения.

С появлением микропроцессорной техники стало возможным массовое производство миниЭВМ, а затем и персональных компьютеров.

Крупные компании и корпорации, которые располагали несколькими компьютерами, старались объединить свои вычислительные ресурсы для совместного использования.

Сетевой режим работы основан в первую очередь на коллективном использовании информационных ресурсов, а вопросы загрузки процессорного времени отошли на задний план. Это стало возможно в связи с резким удешевлением стоимости персональных ЭВМ, развитием их массового производства иувеличением их производительности.

Особенности работы в сети

Технические особенности работы в сети заключаются в следующем:

- основными элементами сети являются отдельные *узлы (хост, host*) – стандартные компьютеры, не имеющие ни общих блоков памятини общих периферийных устройств;
- каждый компьютер работает под управлением собственной операционной системы;
- взаимодействие осуществляется через сетевые адаптеры, линии связи и коммуникационное оборудование.

Организационные особенности работы в сети:

- обеспечивается возможность доступа к разнообразным информационным ресурсам;
- реализуются возможности групповой разработки проектов;
- имеется возможность объединения вычислительных ресурсов отдельных компьютеров сети в единую программно-техническую систему для решения сложных задач;

– взаимодействие многих пользователей приводит к тому, что могут быть сделаны попытки несанкционированного доступа к информации пользователя;

– на компьютер пользователя могут быть установлены злонамеренные программы: вирусы, трояны и проч.;

– информация может быть разрушена, а работа хоста заблокирована;

– может быть считана информация представляющая тайну (государственную, военную, коммерческую, промышленную, персональную и личную).

Основные преимущества работы в сетевом режиме

– пользователь может пользоваться всеми доступными ресурсами других хостов в сети и выходами в глобальные сети;

– пользователю доступны многие сервисы такие ка FTP, Email, служба печати, службы удалённого доступа, ресурсы Интернет, облачные технологии и проч.;

– имеются возможности широкого общения в режиме реального времени: телеконференции, переговоры, сетевые игры, социальные сети, удаленный видеоконтроль и т.п.

Основные характеристики сетей

Доступность (availability) (готовность или коэффициент готовности) определяется как доля времени, в течении которого система может быть использована. Чтобы обеспечить высокую доступность можно использовать дублировать ключевых элементов ситемы. Например, организовать кластеры из нескольких серверов, которые обеспечивали выдачу информации одновременно нескольким пользователям. При этом необходимо обеспечивать зеркальный режим обновления информации на различных устройствах хранения.

Отказоустойчивость (faulttolerance), есть характеристика надёжности составляющих элементов. Иногда под отказоустойчивостью понимают способность системы скрыть от пользователя отказ отдельных её элементов. Но в этом случае, на наш взгляд, следует использовать термин *живучесть*. *Живучесть* означает, что выход отдельных элементов системы не приводит к её полному отказу. Система продолжает выполнять свои функции, пусть даже в более замедленном режиме.

Безопасность (security) определяется как способность системы противостоять несанкционированному доступу. В распределённых системах обеспечение безопасности значительно сложнее, чем в централизованных.

Уязвимость компьютерных сетей связана с использованием линий связи, доступа к коммуникационным линиям, к портам, отдельным узлам.

Оставленные без присмотра компьютеры, несоблюдение правил их размещения, плохая защита при выходе в глобальные сети общего пользования также снижают информационную безопасность сетей. Обеспечение безопасности должно носить *системный* характер.

Расширяемость (*extensibility)* сети предполагает возможность легкого добавления числа элементов (пользователей, компьютеров, приложений, служб), увеличения протяженности сети, замены оборудования более мощным. Например, локальная сеть Ethernet обладает неплохой расширяемостью, но при большом числе хостов в сегменте (более 30-40) значительно снижает производительность.

Масштабируемость (scalability) означает, что имеется возможность увеличение числа хостов и протяженности сети без снижения производительности. Улучшение масштабируемости предполагает включение дополнительного сетевого оборудования, оптимизации структуры сети, повышение производительности путем замены сетевого оборудования.

*Прозрачность(transparency)*сети это пользовательское представление сети как традиционно представляемая конечными пользователями (неспециалистами) единая электронно-вычислительная машина.

Прозрачность означает скрытие сложной структуры сети, сложных технологий обработки сетевых взаимодействий и представление работы в сети в упрощенном виде как работы с локальными ресурсами. На программном уровне прозрачность означает, что для реализации вызовов в сети используются те же вызовы, которые применяются для доступа к локальным ресурсам.

Лекция 2. ЦЕЛИ И ЗАДАЧИ АДМИНИСТРИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Администрирование компьютерных сетей представляет собой организационно-технический процесс управления взаимодействием оборудования компьютерной сети и, в определенном смысле, взаимодействием пользователей сети.

Целью администрирования компьютерных сетей является обеспечение безотказной и безопасной работы компьютерной сети и, в частности, рабочих станций (узлов сети), линий связи, сетевого оборудования, серверных приложений и информационных баз для решения задач обеспечения пользователей необходимой информацией для выполнения их трудовых функций или обеспечения нормальной жизнедеятельности.

Основными функциями администратора (администраторов) компьютерной сети являются:

– обеспечение безотказной работы аппаратного обеспечения и линий связи сети;

– поддержка в актуальном состоянии программного обеспечения на серверных и клиентских узлах;

– обеспечение бесперебойного функционирования информационных ресурсов сети;

– организационно-методическое управление компьютерной сетью;

– определение и предоставление, а также разграничение прав доступа пользователей сети;

– обеспечение защиты от проникновений, несанкционированного доступа и установки злонамеренных программ(вирусов, троянов, шпионов и проч.);

– планирование и проектирование развития сети.

В случае небольшой сети все функции администратора может выполнять один сотрудник – администратор сети. При наличии сети сложной структуры с большим числом пользователей и развитым информационным и программным обеспечением могут созданы группы администраторов с разграниченными функциями.

В этом случае полезно определить функции администраторов следующим образом.

Администратор компьютера – *п*ользователь ответственный за настройку конкретного узла (компьютера) сети. Имеет права вносить изменения в системное и пользовательское программное обеспечение, создавать и изменять локальные учетные записи других пользователей компьютера, права доступа ко всем файлам компьютера.

Администратор домена – пользователь домена, обладающий правами настройки и управления всеми службами домена, ведения учетных записей пользователей и групп домена, присвоения паролей, настройки профилей, управление доступом в рамках домена.

Администратор компьютерной сети – пользователь сети, ответственный за планирование, настройку и управление ежедневной работой сети. Обладает самыми широкими правами доступа к различным подсистемам сети.Администратора сети часто называют также системным администратором.

Администратор кластера – доверенное лицо, ответственное за настройки кластера и его узлов, групп и ресурсов и его функционирование.

Администратор web-узла – доверенное лицо, ответственное за ежедневное бесперебойное функционирование web-ресурсов предприятия, учреждения, организации. Также может выполнять обновление информационных материалов, изменять структуры ресурсов оптимальным образом и проч. В его функции может быть подключено управление FTP-сервером, e-mailит.п.

В современных условиях имеет определенный смысл назначать лиц, *ответственных за информационную безопасность* функционирования компьютерных сетей.

Распределение обязанностей среди членов группы администратором может быть иным.

Стратегии администрирования

В управлении сетями можно выделить следующие стратегические подходы.

1. Администратор на основании целей и задач компьютерной сети и своего личного опыта самостоятельно решает вопросы управления компьютерной сетью и принимает основные решения.

2. Управления компьютерной сетью строго регламентируются руководством организации, предприятия, учреждения. Администратор лишь выполняет данные поручения.

3. Решения управления компьютерной сетью осуществляются администратором с учетом требований конечных пользователей и руководства различного ранга.

4. Администратор делегирует свои полномочия пользователям сети и руководителям подразделений.

Наиболее оптимальной представляется стратегия, включающая элементывсе вышеперечисленные стратегии в некотором сочетании.

Хотелось бы остеречь от ошибок администраторов, которые могут приводить к конфликтам, конфронтации, склокам и другим нездоровым проявлениям в трудовых коллективах.

1.Опыт информатизации различных организаций выявил такое нездоровое явление как «конфликт вице-президентов». Суть этого явления заключается в том, что на начальной стадии информатизации обычно изучались информационные потоки в организации. С этой целью президентом компании отдается приказ всем вице-президентам предоставлять необходимый доступ к информационным потокам вновь назначенному вице-президенту по информатизации. Вполне понятно желание вице-президента по информатизации не только познакомиться с количественными и формальными характеристиками потоков, но с их содержанием. Также велико искушение передать указанную информацию президенту компании. Это сразу же приводит к конфликтной ситуации, в основе которой недоверие, иногда ненависть. Безусловно, это не способствует эффективной командной работе коллектива.

Вывод, *администраторы не должны иметь доступа к конфидициальной информации, непосредственно связанной с деятельностью предприятия. Их задача обеспечить слаженную эффективную работу членов коллектива. При этом доступ к информации должны иметь только лица, которым она необходима для выполнения своих обязанностей.*

Если это условие нарушается, то действия администратора по меньшей мере НЕ СООТВЕТСТВУЮТ*возложенным на него обязанностям и представляют серьёзную угрозу информационной безопасности.*

2. Иногда администратор, отслеживая трафик, приходит к выводу, что некоторые пользователи просматривают информацию, не имеющую отношения к их функциональным обязанностям, накапливает подобную информацию и передает для анализа руководству либо распространяет среди третьих лиц.

Вывод. Это неправильно. Основная функция администратора при поддержке сети предприятия – НЕ ДОПУСТИТЬ несанкционированного использования сети предприятия.

Администратор уже на первой стадии запуска сети в работу должен был предусмотреть и ограничить с помощью аппаратных и программных средств, имеющихся в его распоряжении, доступ к ресурсам сети, которые соответствуют целям и задачам сети предприятия.

Согласно, действующему законодательству и общепринятым нормам морали, сбор, накопление, хранение и распостранение личной информации преследуется по закону и осуждается обществом. Более того, негласное

видеонаблюдение и прослушивание может быть только в случае,если возбуждено уголовное дело и имеются определенные законом санкции.

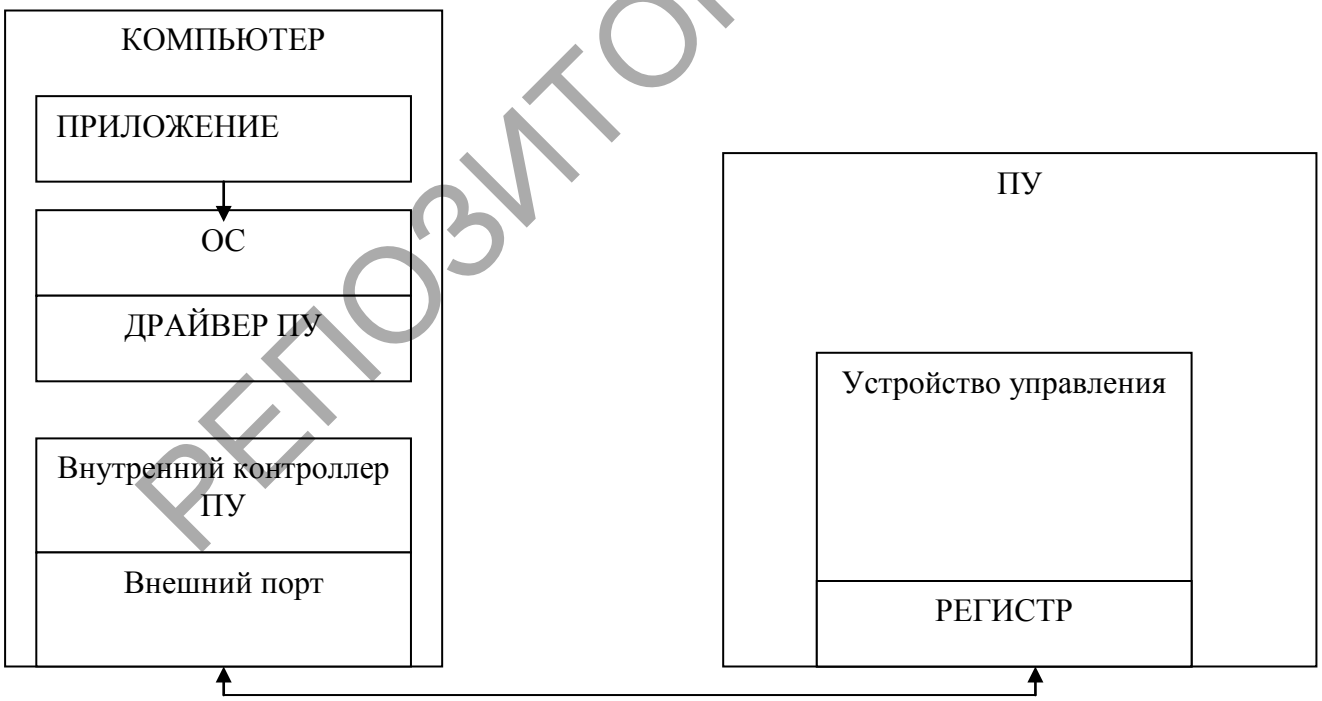
Тем не менее, жизнь всегда богаче наших представлений. Так, если администратор заметил, что действия пользователей могут в некоторой степени повредить эффективной работе предприятия, функционированию сети или нарушают правила внутреннего распорядка и правила пользования сетью, то у него есть возможность немедленно прервать процесс доступа и ограничить доступ к данному ресурсу либо для конкретного пользователя, группы или всем пользователям сети. Выполнение своих обязанностей администратора, регулярно и добросовестно, позволит в кратчайшие сроки обеспечить дисциплину использования сети и качество сетевой работы сотрудников.

Следует также помнить, что исследования использования сетевых ресурсов указывают, что слишком жесткие ограничения не способствуют росту производительности труда и укреплению здоровых отношений среди сотрудников.

Лекция3.ВЗАИМОДЕЙСТВИЕ КОМПЬЮТЕРОВ В СЕТИ

Взаимодействие компьютера с периферийными устройствами

Для обеспечения обмена информацией между компьютером (ПК) и периферийными устройствами (ПУ) предусмотрена линия связи и набор правил обме-



на – интерфейс. Стандартными средствами являются параллельный интерфейс Centronics и последовательный интерфейс RS-232C. Для указанных целей также могут использоватьсяи другие интерфейсы общего назначения: USB, USB 2.0, USB 3.0, IEE и др., а также специализированные интерфейсы, предназначенные для обмена со специальной аппаратурой.

Интерфейсы реализованы со стороны ПК контроллерами ПУ и соответствующими драйверами.

Обмен информацией происходит следующим образом.

Приложение генерирует запрос на передачу информации для выполнения ПУ и обращается в ОС, которая передает запрос на выполнение драйверу устройства. Драйвер формирует набор высокоуровневых команд организации работы ПУ и передаёт контроллеру ПУ. Внешний порт получает от контроллера ПУ поток низкоуровневых команд и передает сформированный сигнал на регистр устройства управления ПУ. Синхронизация передачи сигнала обеспечивается передачей стартового и стопового сигналов в начале и конце передачи.

Контроль достоверности передачи может обеспечиваться формированием драйвером бита контроля четности или передачей соответствующей контрольной суммы. Обычно приложение, ОС, драйверы решены изготовителем оборудования программно, а программы контроллера и устройства управления аппаратно, что взначительной степени повышает скорость обработки.

Простейший пример взаимодействия двух компьютеров.
Понятие о технологии «клиент-сервер».

Технология «клиент-сервер» основана на придании функций клиента (управление) одному устройству, а обслуживающие функции (серверные другому). Обмен информацией осуществляется следующим образом.клиент формирует и передает сообщение о получении необходимой информации серверному устройству. Сервер, получив задание, отыскивает и обрабатывает необходимую информацию, формирует ответ в оптимальном виде, и пересылает результат клиенту. Такая технология взаимодействия позволяет освободить сетевые линии связи от пересылки больших массивов информации и ограничиться трафиком запросов и ответов. Кроме этого, при использовании технологии взаимодействия в сети «клиент-сервер» основная нагрузка по поиску и обработке информации возлагается на серверное устройство и к нему предъявляются повышенные требования по производительности. Клиентские устройствав этом случае могут обладать невысокой производительностью. Это приводить к экономии материальных затрат при реализации клиент-серверных технологий в сетях различного уровня.

Одноранговая и доменная структура сети.

На начальных этапах объединения небольшого количества (2-5) узлов в сеть использовалась однорангавая структура. Такая сеть состояла из узлов, каждый из которых являлся одновременно и клиентом (управление) и сервером (обслуживание). Это позволяло достаточно эффективно осуществлять обмен информацией в сети. Такие сети могут быть использованы в небольших сетях. При этом их реализация обычно выполняется между доверенными клиентами. При большом количестве участников сетевого взаимодействия возникают серьезные проблемы информационной безопасности (опасность несанкционированного доступа, потери и разрушения информационных баз и проч.).

Для обеспечения устойчивой и безопасной работы в сети разработана и используется доменная структура сетевого взаимодействия. В этом случае совокупность узлов сети (т.е. компьютеров, объединенных линиями связи) объединяются в отдельные подмножества, называемыми доменами. Эти домены предназначены для решения общих задач. Для управления в пределах домена служит устройство, которое обеспечивает функции управления доменами – контроллер домена. Иногда в домене могут быть созданы два или более контроллеров, работа которых синхронизируется. Включение несколько контроллеров в домен может происходить по причинам повышения информационной безопасности и(или) территориальной разобщенности доменной сети. В первом случае выход из строя контроллера сети никак не скажется на ее работоспособности с точки зрения пользователя, так как функции контроллера дублируются. Во втором случае при значительной удаленности отдельных подмножеств узлов домена их управление реализуется ближайшим контроллером, который все изменения хранимой информации в течении нескольких минут передает на другой контролер, тем самым обеспечивают синхронизацию управления доменом с несколькими контроллерами.

Лекция 4. МОДЕЛИ СЕТЕВЫХ ВЗАИМОДЕЙСТВИЙ

В процессе создания и развития систем сетевого взаимодействия возникла настоятельная необходимость в унификации и стандартизации.

Практика создания локальных, корпоративных, региональных и глобальных сетей породила множество правил взаимодействия в сетях. Они были реализованы программно и аппаратно и выполняли функции преобразования информации при подготовке к передаче и обратного преобразования при приеме.

Эти правила получили названия протоколов. Протоколы могут быть реализованы с помощью различных программ, но их функции должны быть стандартными, а входные и выходные сигналы должны иметь одинаковую унифицированную структуру.

В результате анализа множества протоколов взаимодействия в сетив 1983 году была разработана Международнойорганизациейпостандартизации (InternationalOrganizationforStandardization, ISO) на основемодели взаимодействия открытых систем (Open System Interconnection) был разработан соответствующий стандарт. Этот стандарт предусматривал представление протоколов в виде семи групп – уровней:

- физический уровень (PhysicalLevel);
- канальный уровень (DataLinkLevel);
- сетевой уровень (NetworkLevel).
- транспортный уровень (TransportLevel).
- сессионный уровень (SessionLevel).
- представительский уровень (PresentationLevel).
- уровень приложения (ApplicationLevel).

Самый низкий - физический уровень определял требования к формированию электрических сигналов, которые передавались в линии связи и интерфейсы

устройств. Остальные уровни предполагали обработку и формирование сообщений с целью их подготовки к передаче и формированию сигналов на физическом уровне.

Все уровни связаны последовательной обработкой сообщений вплоть до формирования электрического сигнала. При приёме сигнала происходит последовательная обработка сигнала, начиная с физического уровня до уровня приложения в противоположном порядке.

Все уровни выполняют согласованную обработку сообщений, используя сервисы предыдущего уровня и предоставляя свои сервисы последующему уровню.

Таблица 1.1. *Уровни сетевой модели OSI*

Уровень	**Название**	**Описание**
1.	Физический уровень	Отвечает за физическое подключение компьютера к сети. Определяет уровни напряжения, электрические параметры импульсов, параметры кабеля, разъемы, распайку проводов и т. п. В настоящее время реализуется аппаратно.
2.	Канальный Уровень	Подготавливает данные для передачи (разбивая их на кадры определенной структуры) и преобразует обратно во время приема (восстанавливая из кадров). Реализуется аппаратно.
3.	Сетевой уровень	Обеспечивает маршрутизацию данных в сети
4.	Транспортный уровень	Обеспечивает последовательность и целостность передачи данных
5.	Сессионный уровень	Устанавливает и завершает коммуникационные сессии
6.	Уровень представления	Выполняет преобразование данных и обеспечивает передачу данных в универсальном формате
7.	Уровень приложения	Осуществляет интерфейс между приложением и процессом сетевого взаимодействия

На каждом уровне блоки информации имеют собственное название

Название блока информации в модели

Уровень	*Название уровня*	*Название блока информации*
1	Физический уровень	Бит
2	Уровень данных	Кадр (пакет)
3	Сетевой уровень	Датаграмма
4	Транспортный уровень	Сегмент
5, 6, 7	Уровень приложения	Сообщение

Спецификации OSI, хотя являются международным стандартом, тем не менее представляют теоретический интерес и в практике не используются в силу сложности многоуровневой классификации и в силу того, что при их разработки слабо учитывался наработанный опыт и существенные потребности практики.

Терминология

Базовые сетевые термины

Термин	*Определение*
Датаграмма	Пакет данных, который представляет единицу информации при сетевом обмене
DNS (Domain Name Service, служба, сервердоменныхимен)	Программа, которая обеспечивает поиск цифрового адреса для соответствующего символического имени хоста (т.е. разрешает символическое имя в цифровой адрес). Иногда может быть использована для выполнения обратной операции.
Интернет	Глобальная компьютерная сеть, которая реализована на семействе протоколов TCP/IP
FTP (File Transfer Protocol, протоколпередачифайлов)	Протокол приема и передачи файлов между двумя компьютерами
IP (Internet Protocol, протокол Интернет)	Основа семейства протоколов TCP/IP. Практически любой протокол из этого семейства базируется на протоколе IP
ICMP (InternetControlMessageProtocol, протокол управляющих сообщений в стеке протоколов IP)	Используется для передачи управляющих сообщений протокола IP
NFS (Network File System, сетевая файловая система)	Система виртуальных дисков, позволяющая клиентским компьютерам использовать каталоги сервера в качестве диска
NIC (Network Information Center, сетевой информационный центр)	Международная организация,отвечающая за выполнение административных функций и раздачу сетевых адресов и имен
Узел (Node, Host)	Устройство (компьютер, принтер, камера и др.) в сети, которое имеет хотя бы один сетевой адрес и которое участвует в сетевом взаимодействии непосредственно.
OSI (OpenSystemInterconnection, взаимодействие открытых систем)	Модель взаимодействия открытых систем
RIP (RoutingInformationProtocol, протокол маршрутизации	Протокол, который используется для обмена информацией между маршрутизаторами

информации)	
SMTP (SimpleMailTransfer-Protocol, простой протокол передачи электронной почты)	Протокол обмена электронной почтой
SNMP (Simple Network Management Protocol, простой протокол управления сетью)	Протокол управления сетевыми устройствами
TCP (Transmission Control Protocol, протокол управления передачей)	Протокол надежной передачи данных
Telnet	Протоколудаленного сетевого подключения к компьютеру, который эмулирующее терминал
UDP (UserDatagramProtocol, протокол пользовательских датаграмм)	Протокол обмена блоками информации без установки соединения

Модель сетевого взаимодействия TCP/IP

Архитектура семейства протоколов TCP/IP (TransmissionControlProtocol/ InternetProtocol), протокол управления передачей/интернет-протокол) основана на представлении, что коммуникационная инфраструктура содержит три вида объектов: процессы, хосты и сети.
Основываясь на этих трех объектах, разработчики выбрали четырехуровневую модель:
Уровень сетевого интерфейса (NetworkInterfaceLayer).
Уровень межсетевого интерфейса — Интернета (InternetLayer).
Транспортныйуровень (Host-to-Host Layer).
Уровень приложений/процессов (Application/ProcessLayer).

Сопоставление сетевых моделей OSI и TCP/IP
Нетрудно заметить, что модель TCP/IP отличается от модели OSI.

Соответствие модели TCP/IP и модели OSI

TCP/IP	OSI
Уровень приложений	Уровень приложений
	Уровень представления
	Уровень сеанса
Транспортный уровень	Транспортный уровень
Межсетевой уровень (Интернет)	Сетевой уровень
Уровень сетевого интерфейса	Уровень канала данных
	Физический уровень

Как видно из таблицы, уровень сетевого интерфейса модели TCP/IP соответствует сразу двум уровням модели OSI, а уровень приложений модели TCP/IP — трем уровням модели OSI.

3. ПРАКТИЧЕСКИЙ РАЗДЕЛ

Лабораторная работа 1. Проектирование корпоративных сетей

Цель работы: Изучение основных требований к корпоративным компьютерным сетям и содержание этапов проектирования.

Теоретические сведения.

Корпоративной называют компьютерную сеть масштаба крупнейшего предприятия или объединения нескольких предприятий в корпорацию. Такая сеть представляет обычно несколько локальных сетей, объединенных в крупнейшую сеть, обслуживающую нужды корпорации. Отдельные сегменты сети могут быть связаны непосредственно либо с помощью средств удаленного доступа. Важными особенностями корпоративных сетей являются:

1. Относительно самостоятельное функционирование отдельных сегментов корпоративной сети;
2. Возможность раздельного управления сегментами;
3. Наличие автономных хранилищ информации;
4. Наличие разграниченной подсистемы управленияобщим доступом к информационным ресурсам;
5. Необходимость оперативной координации работы сегментов.

Планирование корпоративной сети предполагает:

- анализ организационной структуры корпорации (предприятия);
- определение и конкретизация цели и задач корпоративной сети;
- определение общих требований к сети в целом и отдельным её сегментам;
- сбор данных и анализ имеющегося аппаратного обеспечения (компьютеров, линий связи, сетевого оборудования);
- планирование физической структуры корпоративной сети в соответствии с заданием;
- планирование логической структуры корпоративной сети;
- определение примерного состава оборудования;
- верификация сети с точки зрения информационной безопасности.

Задание лабораторной работы.

1. Разработка примерной локальной сети Дворца культуры.
2. Разработка примерной локальной сети театра.
3. Разработка примерной локальной сети библиотеки.
4. Разработка примерной локальной сети крупного музея.
5. Разработка примерной локальной сети концертного зала.
6. Разработка примерной корпоративной сети управления культуры.

Лабораторная работа 2.Обеспечениевзаимодействияв сетях

Цель работы: Рассмотреть средства и технологии обеспечения эффективного взаимодействия компьютерных узлов в сети

Теоретические сведения

Сетевые протоколы

Протоколы межсетевого уровня (Интернет)

Протоколы межсетевого уровня (Интернет) являются базовыми в семействе протоколов TCP/IP. Перечислим их названия: TCP/IP, ARP/RARP и ICMP.

Протокол IP

Первоначальный стандарт IP разработан в конце семидесятых годов и не предусматривал работу с огромным количеством хостов, которое существует в всовременном Интернете. В этой связи в настоящее время утвержден новый стандарт IP IPv6. Однако скорейшему внедрению этому протоколу мешает находящееся в эксплуатации значительное количество количества программных и аппаратных средств, не приспособленных для работы с IPv6, поэтому его внедрение производится постепенно.

Обмен информацией в Интернете обеспечивается с помощью пакетов.

Формат пакета IPv4

Структура пакета IPv4включает заголовок и поле данных. Поле данных не имеет структуры и определятся только размером (до 65 535 байт). Однако при передаче Длина пакета определяется с учетом длины пакета физического уровня данной сети. В сетях критерием является максимальный размер поля данных кадра в который следует помещать передаваемый пакет. Эту длину называют единицей транспортировки (MaximumTransferUnit, MTU). Например, для сетей Ethernet длинаMTUравна 1500 байт, сети FDDI— 4096 байт.

поле Длина заголовка (HLEN) пакета IP. Для него отводится 4 битав которых указывается значение длины заголовка (в 32-битовых словах). Чаще всего-

заголовок имеет длину в 20 байт (пять 32-битовых слов).При необходимости длина может быть увеличена за счет поля Резерв (IP OPTIONS);

поле Тип сервиса (SERVICE TYPE) имеет размер в 1 байт, в котором определяется приоритетность пакета, а также вид критерия выбора маршрута. Первые три бита указывают на приоритет пакета (PRECEDENCE), который принимает значения от 0 (нормальный пакет) до 7 (пакет управляющей информации). ПодполеТип сервиса также содержиттри бита, которые определяют критерий выбора маршрута (бит D (delay) указывает на выбор маршрута с минимизацией задержки доставки данного пакета, бит T — доставка с максимизацией пропускной способности, а бит R — доставка с максимумом надежности);

поле Общая длина (TOTAL LENGTH) содержит 2 байта и определяет общую длину пакета (заголовок и поле данных);

поле Идентификатор пакета (IDENTIFICATION) имеет длину 2 байта и предназначено для распознавания пакетов, которыеформируются в результате фрагментации исходного пакета. Для всех фрагментов исходного пакета значение поля одинаково;

поле Флаги (FLAGS) имеет длину 3 бита и указывает на допустимость фрагментации пакета (бит DonotFragment, DF — запрещает фрагментацию данного пакета, бит MoreFragments, MF — указывает на то, что пакет переносит промежуточный фрагмент);

поле Смещение фрагмента (FRAGMENT OFFSET) имеет длину 13 бит, оно применяется для определения смещения (в байтах) поля данных от начала поля данных исходного пакета, который был фрагментирован. Это необходимо для сборки/разборки фрагментов при их передачах в сетях;

поле Время жизни (TIME TO LIVE) имеет длину 1 байт и содержит информацию в секундах об оставшемся времени жизни, в течение которого пакет может перемещаться по сети. Время жизни устанавливается источником передачи и уменьшается на единицу в каждом узле сети и даже при транзитной передаче. По истечении времени жизни пакет не ретранслируется (аннулируется);

поле Идентификатор протокола верхнего уровня (PROTOCOL) имеет размер в 1 байт и определяет протоколу верхнего уровня данного пакета (TCP, UDP или RIP);

поле Контрольная сумма (HEADER CHECKSUM) имеет размер 2 байта и указывает длину заголовка;

поля Адрес источника (SOURCE IP ADDRESS) и Адрес назначения (DESTINATION IP ADDRESS) имеют размер (32 бита) каждое и одинаковую структуру;

поле Резерв (IP OPTIONS) применяется обычно при отладке сети и является необязательным. Это поле может содержать несколько подполей предопределенных типов.

Протокол IPv6

Появлению IPv6 имелись серьезные предпосылки:

- протокол IPv4 разработан без учета особенностей современной сетевой инфраструктуры и нагрузочных характеристик;

- необходимость использования данных в реальном времени (звук, видео). Передача этой информации очень чувствительна к задержкам передачи пакетов, особенно с учетом их очень больших объемов;

- весьма значительное расширение сети Интернет и соответственно истощение 4 байтовых адресов. Механизмы компенсации не решают проблему кардинально.

В основе протокола IPv6 соблюдаются неизменными основные принципы IPv4.

Сохранено следующее:

- датаграммный принцип работы;

- фрагментация пакетов;

- разрешение устанавливать максимальное время жизни пакета отправителем.

Наиболее важные отличия протокола заключаются в следующем.

- использование цифровой адресации длиной в 16 байт (128 бит);

- использование гибкого формата заголовка (в IPv6 используется базовый формат заголовка фиксированного формата и набор заголовков различного формата, которые не являются обязательными;

- поддержка резервирования пропускной способности;

- поддержка расширяемости протокола (в случае необходимости существует возможность включения дополнительных функций.

Адресация в IPv6

Протокол IPv6 имеет длину адреса 128 бит или 16 байт.
Для обеспечения преемственности с адресацией версии IPv4 в IPv6 предусмотрен класс адресов, который содержит 0000 0000 в старших битах адреса. При этом предусматривается, что младшие 4 байта адреса этого класса содержат адрес IPv4. Современные маршрутизаторы, которые поддерживают обе версии адресов, обеспечивают трансляцию адресов из IPv4 и наоборот.

В IPv6 предусмотрено обобщение типов адресов версии 4 в следующие обобщеные типы:

Unicast — индивидуальный адрес. Определяет отдельный узел — компьютер или устройство. При этом предусматривается доставка пакетов по кратчайшему маршруту;

Cluster — адрес кластера. Кластер – это группа узлов, имеющих общий адресный префикс. При этом пакет передается по кратчайшему маршруту ближайшему узлу в кластере;

Multicast — адрес набора узлов. Копии пакета доставляются каждому узлу в наборе.

Адреса в версии IPv6 подразделяются на классы, которые определяются значениями старших битов адреса. Значительная часть классов зарезервирована для будущего применения.

Новым представляющим интерес для практического использования, является класс, который предназначен для провайдеров услуг Интернета (Provider-AssignedUnicast).

Протоколы маршрутизации

Протоколы маршрутизации можно подразделять на протоколы внутреннего шлюза (InteriorGatewayProtocol, IGP) и протокол внешнего шлюза (ExteriorGatewayProtocol, EGP).

Протокол внутреннего шлюза предназначен для управления процессом маршрутизации в пределах автономных сетей (сети или сетей одного владельца), для которых определены внутренняя структура и точки взаимодействия с окружением.

Протокол внешнего шлюза обеспечивает маршрутизацию между автономными системами.

Следующие протоколы маршрутизации нашли широкое применение в настоящее время:

RIP (Routing Information Protocol) — протоколданныхмаршрутизации. Этот протокол получил широкоераспостранение в основном из-за стандартной утилиты routedдля UNIXоперационных систем.

OSPF (OpenShortestPathFirst) — протокол промышленного уровня для определения кратчайшего пути;

IGRP (InteriorGatewayRoutingProtocol) — протокол внутреннего шлюза для маршрутизаторов CISCO;

BGP (BorderGatewayProtocol) — протокол граничного шлюза. Выполняет маршрутизацию в сложных топологиях и имеет настройки стратегии маршрутизации;

DVMRP (VectorMulticastRoutingProtocol) — протокол групповой маршрутизации по вектору расстояния.

Адресация в TCP/IP

Для любого сетевого устройства в сети IP определены три адреса.

На уровне локальной сети (например, Ethernet) используется MAC-адрес сетевого адаптера (*MediaAccessControl)*, который должен быть уникальным, хотя бы внутри локальной сети. Изначально предполагалось, что уникальность MAC-адреса сетевого устройства обеспечивается производителем. В частности, его длина 6 байт, из которых 3 первых байта представляют уникальный код производителя, а три младших байта назначаются производителем также уникальным образом. Но производители, часто предоставляют средства для изменения MAC-адреса и следовательно при создании локальной сети и ее эксплуатации администратору необходимо озаботиться тем, чтобы узлы в сети имели

уникальные MAC-адреса. В процессе функционирования доменной сети узлам сети присваиваются IP-адреса (4-х байтовые или 16-ти байтовые) с помощью сервера DHCP (DynamicHostConfigurationProtocol) автоматически либо администратором. Ясно, что во избежание некорректности функционирования сети этот адрес также должен быть уникальным. Это также забота администратора. Обращение к компьютеру обычно в доменной сети происходит по цифровому IP-адресу. Но внутри локальной сети взаимодействие предполагается на канальном уровне и для этого необходимо использовать MAC-адреса. Для разрешения IP-адреса в MAC- адрес используется протокол ARP (AddressResolutionProtocol (сети IPv6 используется протокол ICMPv6 (InternetControlMessageProtocolfortheInternetProtocolVersion 6).

На прикладном уровне (например: в браузерах, электронной почте, приложениях FTP и проч.) широко используются удобные для человека символьные адреса (например: www.yandex.ru). Однако, при пересылке пакетов в них отсутствуют символьные адреса, а используются только цифровые.

Для разрешения символьного адреса в IP-адрес используется специальный DNS-сервер (DomainNameServer), который отыскивает в свой базе символьное имя и возвращает цифровой адрес.

Создание символьного имени подчиняется определеным правилам. В частности, символьное имя может быть сложным. Например:www.mininform.gov.by/. В этой структуре имеются следующие части: указание на машину.ДоменноеИмя3уровня.ДоменноеИмя2уровня.ДоменноеИмя1уровня.

Если при поиске DNS-сервер не обнаружит символьное имя в своей базе, то он обратится к базе DNS по имени 2 уровня и проверит, зарегистрирован ли данный клиент в его базе. В случае если клиент с доменным именем не обнаружен или в его базе отсутствует клиент с именем 3 уровня, то это неправомочное имя. В противном случае, DNS-сервер найдет разрешение символьного имени в IP-адреси зафиксирует эти сведения в своей базе для дальнейшего использования.

Всегда IP-адреса записывают в виде десятичных чисел, которые разделены точками. В IPv4 существует несколько классов сетей для определенных интервалов адресов.

Распределение сетевых адресов по классам сетей

Класс	Первый байт	Формат	Комментарии
A	1-126	с.м.м.м	Соответствует очень большим сетям: региональным, большие корпорации, крупные провайдеры.
B	128-191	с.с.м.м	Крупные сети--большие фирмы, большие интернет-провайдеры.
C	192-223	с.с.с.м	Локальные сети на 254 компьютера
D	224-239	—	Подсети, выдаваемые провайдерами

E	240-254	—	Экспериментальные адреса

Для получения IP-адресов следует обратиться в международную службу регистрации информационного центра InterNIC. Однако небольшое количество адресов можно получить практически у любого интернет провайдера.

Надо отметить, что часть адресов предназначена для использования только в локальных сетях:

10.0.0.0 - 10.255.255.255 (класс A)

172.16.0.0 - 172.31.255.255(класс B)

192.168.0.0 - 192.168.255.255(класс C)

Существуют IP-адреса, которые имеют специальное значение:

адрес, в котором сетевая часть содержит нули, соответствует хосту в локальной сети. Например, 0.0.0.23 соответствует 23 рабочей станции в данной локальной сети, адрес 0.0.0.0 соответствует текущейрабочей станции;

адрес 127.X.X.X представляет собой фиктивную сеть, которая не имеет никаких аппаратных сетевых интерфейсов и представляет только текущий локальный узел. Адрес 127.0.0.1 всегда обозначает текущийузел с символическим именем localhost;

адрес, который содержит число 255, является широковещательным, который будет рассылать пакеты по другим адресам для всего множества из 255 компьютеров.

Задание лабораторной работы.

Спланировать доменные имена для разработанной в лабораторной работе 2 или предложенной преподавателем примерной физической структуры сети в соответствии с правилами именования узлов сети.

Лабораторная работа 3.Установка и настройка сервера сети

Цель работы: Изучить основные способы подготовки сетевых компьютеров и дистрибутивов для установки серверных операционных систем и восстановления системного программного обеспечения.

Теоретические сведения.

Изучить и рассмотреть особенности полной переустановки сетевой операционной системы и обновления устаревшей ОС.

Рассмотреть способы полной переустановки сетевой операционной системы (с системного диска в диалоговом режиме, с системного диска с использованием файла ответов, с использованием метода клонирования с помощью утилиты SysPrep).

Законспектировать теоретические сведения.

Задание лабораторной работы.

1. *Выполнить переустановку операционной системы*
2. *Разработать сценарий установки с использованием файла ответов*

Лабораторная работа 4.Создание нового домена

Цель работы: Изучение установки и первичной настройки операционной системы MSWindowsServer(установка и администрирование DNS, службы каталогов ACTIVEDIRECTORY исервера WINS)

Теоретические сведения

При создании нового домена следует выполнять следующие рекомендации по именованию доменов и поддоменов.

1. *Количество уровней домена должно быть не более 5.*
2. *Все имена доменов и поддоменов должны быть уникальными.*
3. *Следует использовать простые, общепринятые, интуитивно-понятные имена.*
4. *Помните, что регистр символов в именах доменов не учитывается. Избегайте длинных имен.*
5. *Согласно стандарту RFC 1035 в именах допустимо использование следующих символов A–Z, a–z и дефис «-«.*
6. *DNS-сервер фирмыMicrosoft поддерживает символы Unicode, что позволяет использовать при именовании шрифты национальных алфавитов. Однако, следует помнить, что использование национальных алфавитов возможно в сети для которой все серверы и клиенты также поддерживают символы Unicode* (например, установлены операционные системы WindowsXP и выше).

При подготовке к лабораторной работе следует законспектировать следующий материал.

1. *Понятие зоны, типы зон, зоны прямого и обратного просмотра. Их назначение.*
2. *Файл зоны. Синтаксис записей зон. Записи хостов и альтернативных имен.*
3. *Записи серверов.*

Задание лабораторной работы

1. *Спланировать пространство имен DNS структуры сети.*
2. *Спланировать DNS-зоны*
3. *Спланировать DNS-серверы*
4. *Определить порядок взаимодействия с другими DNS-серверами*
5. *Установить и выполнить начальную настройку DNS-сервера сети.*

Лабораторная работа 5.Управление ActiveDirectory

Цель работы: Освоение процесса регистрация пользователей и др. объектов в службе каталогов и основные функции настройки службы.

Теоретические сведения

При подготовке к выполнению лабораторной работы следует изучить и законспектировать:

1. *Концепция Active Directory и структура.*
2. *Пространство имен. Понятия объекта, организационной единицы, домена, дерева, леса, схемы.*
3. *Планирование структуры Active Directory.*

Задание лабораторной работы

1. *Спланировать пространство имен*
2. *Планирование структуры организационных подразделений (объектная модель, географическая, по задачам, по отделам, по проектам).*
3. *Установить и произвести первичную настройку ActiveDirectory.*
4. *Установит и произвести первичную настройку DNS/*

Лабораторная работа 6.Управление доменомWindowsServer

Цель работы: Изучить эффективные методы управления доменом WindowsServer. Изучение методов планирования и управления дисковыми и файловыми ресурсами.

Теоретические сведения.

При подготовке к выполнению работы необходимо изучить теоретический материал и законспектировать:

1. *Свойства домена, изменение режима работы домена, понятие хозяев операций и приемы работы.*

2. *Управление пользователями, создание, копирование, настройка и удаление учетных записей.*
3. *Управление контактами, группами, компьютерами, принтерами, общими папками.*

Задание лабораторной работы.

Выполнить

1. *Создать несколько учетных записей пользователей домена.*
2. *Организовать ОП по двум различным признакам.*
3. *Произвести настройку полученных групп.*
4. *Произвести настройку компьютеров.*

Лабораторная работа 7.Администрирование DHCP

Цель работы: Изучение основных функций планирования и эффективное управление адресным пространством

Теоретические сведения

При подготовке к работе изучить и законспектировать

1. *Основные сведения о протоколе и базе данных DHCP*
2. *Рассмотреть параметры и планирование DHCP-серверов.*

Задание лабораторной работы

При выполнении:

1. *Создать службу DHCP*
2. *Произвести начальную настройку DHCP-сервера.*
3. *Практически изучить автоматическое распределение IP-адресов при подключении и отключении рабочих станций. Описать в отчете.*

Лабораторная работа 8.Управление профилями пользователей

Цель работы: Разработка различные моделей профилей пользователей и изучение способов их организации в группы. Создание и использование.

Теоретические сведения

При подготовке следует изучить:

1. *Понятие профиля пользователя.*
2. *Виды профилей: локальный, перемещаемый и фиксированный*
3. *Методы создания профилей*
4. *Порядок использования профилей*

Задание лабораторной работы

Для выполнения лабораторной работы:

1. *Создать собственный локальный профиль на рабочем месте. Определить основные свойства профиля (логин, пароль, фон рабочего стола, пробные файлы в «Мои документы» и на рабочем столе).*
2. *На основе локального профиля создать перемещаемый профиль, который сохранить в папке \\server\profiles\%username%.*
3. *Войти в перемещаемый профиль, выполнить изменения в настройках, выйти. Зайти в перемещаемый профиль с другого компьютера и убедиться в сохранении сделанных изменений.*
4. *Создать обязательный профиль для пользователя.*
5. *Рассмотреть процедуры создания перемещаемых профилей из профиля по умолчанию, тестового профиля и профиля для всех.*
6. *Описать в отчете.*

Лабораторная работа 9. Настройка групповых и локальных политик

Цель работы: Изучение принципов планирования и процесса настройки групповых и локальных политик.

Теоретические сведения

Изучить и законспектировать:

1. *Понятие и концепции групповых политик*
2. *Рассмотреть шаблоны групповых политик*
3. *Изучить порядок применения групповых политик*

Задание лабораторной работы

Необходимо выполнить:

1. *Ознакомиться с параметрами шаблонов политики безопасности.*
2. *Рассмотреть имеющиеся шаблоны групповых политик.*
3. *Описать основные ограничения политик безопасности.*

Лабораторная работа 10. Эксплуатация компьютерных сетей масштаба предприятия

Цель работы: Изучение эффективных методов управления надежной работой сети масштаба предприятия.

Теоретические сведения

Изучить и составить конспект:

1. *Суть, цель, задачи аудита ресурсов и событий.*
2. *Активизация и настройка службы аудита.*

Задание лабораторной работы

Выполнить:

1. *Базовую настройку аудита на рабочих станциях и сервере сети.*
2. *Проанализировать результаты аудита и сделать выводы по оптимизации взаимодействия.*

Лабораторная работа 11. Администрирование компьютерных сетей под управлением unix-подобных ОС

Цель работы: Изучение особенностей организации и управления сетями на основе Unix-подобных операционных систем

Теоретические сведения

Изучить и законспектировать:

1. *Правила конфигурирование сетевых интерфейсов.*
2. *Изучить структуру и правила настройки proxy-сервера Squid.*
3. *Рассмотреть установку и базовые настройкисерверовDHCP, DNS, NIS, LDAP.*

Задание лабораторной работы

Выполнить:

1. *Подключение новых пользователей и создание соответствующих учетных записей.*

2. *Настроить свойства учетных записей.*
3. *Рассмотреть службы аудита событий и сканирования трафика.*

Лабораторная работа 12. Обеспечение информационной безопасности в сетях

Цель работы: Принципы, методы и средства обеспечения безопасности при эксплуатации компьютерных сетей масштаба предприятия.

Теоретические сведения

1. *Структура управления безопасностью сети.*
2. *Методы и средства анализа защищенности.*

Задание лабораторной работы

1. *Рассмотреть средства мониторинга безопасности в сетях.*
2. *Описать результаты.*

4. РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

Вопросы к зачету

для студентов специализации "информационные системы в культуре"

1. Основные понятия компьютерных сетей. Эволюция режимов работы компьютерных систем. Особенности работы в сетевом режиме.
2. Основные характеристики сетей: доступность *(availability)*, отказоустойчивость *(faulttolerance)*, безопасность *(security)*, расширяемость *(extensibility)*, масштабируемость *(scalability)*, прозрачность *(transparency)*.
3. Цели и задачи администрирования компьютерных сетей.
4. Взаимодействие компьютера с периферийными устройствами. Простейший пример взаимодействия двух компьютеров. Понятие о технологии «клиент-сервер».
5. Модель взаимодействия открытых систем (OpenSystemInterconnection, OSI).
6. Стандартные стеки коммуникационных протоколов: стек OSI, стек TCP/IP (TransportControlProtocol/InternetProtocol), стек IPX/SPX (InternetworkPacketExchange/SequencedPacketExchange), стек NetBIOS/SMB (NetworkBasicInput/OutputSystem/ServerMessageBlock).
7. Основные топологии физических связей при объединении нескольких компьютеров в сеть: полносвязная, общая шина, звезда, кольцо. Особенности их функционирования.
8. Проблема адресации компьютеров в сети. Задачи адресации. Три схемы адресации узлов сети: аппаратные, числовые и символьные адреса.
9. IP- и IPX-адреса. Классы IP-адресов (*версияIPv4*). Особые IP-адреса. Использование масок в IP-адресации.
10. Служба DHCP*(DynamicHostConfigurationProtocol):* назначение, основные функции, принцип действия. Статические и динамические методы распределения IP-адресов.
11. Символьные имена узлов. Службы разрешения имен. Централизованный и распределенный подходы к разрешению имен: особенности функционирования.
12. Реализация NetBIOS-имен. Служба WINS: назначение и принципы действия.
13. Доменная система именования. Сервер DNS (DomainNameSystem): назначение, принципы действия, организация.
14. Линии связи и их классификация. Типы линий связи: проводные, кабельные (медные и оптоволоконные), наземная и спутниковая радиосвязь.
15. Передача сигналов по линиям связи. Аналоговая модуляция и цифровое кодирование.
16. Методыаналоговоймодуляции: амплитудная (AmplitudeModulation, AM), частотная *(FrequencyModulation, FM)*, фазовая*(PhaseModulation, FM)*, квадратурнаяамплитудная (QuadratureAmplitudeModulation, QAM).
17. Цифровое кодирование. Основные способы дискретного кодирования данных: потенциальный код NRZ, биполярный код, биполярный импульсный код, манчестерский код, потенциальный код 2B1Q.
18. Улучшение потенциальных кодов путем использования методов логического кодирования на основе применения избыточных кодов и скрэмблирования.
19. Методы коммутации абонентов. Основные свойства сетей с коммутацией каналов. Принципы коммутации пакетов. Коммутация сообщений.

20.Повторители, концентраторы и сетевые адаптеры: основные функции и технические характеристики.

21.Принципы работы мостов и коммутаторов. Логическая структуризация сети.

22.Классическиетехнологиивзаимодействияузловвлокальныхсетях: Ethernet, Token Ring, FDDI *(Fiber Distributed Data Interface)*.

23.Основные разновидности коммутаторов. Коммутация «на лету» и с буферизацией.

24.Виртуальные локальные сети. Типовые схемы применения коммутаторов в локальных сетях.

25.Маршрутизация в глобальных сетях. Принципы действия маршрутизаторов. Шлюзы. Основные функции.

26.Корпоративная сеть как совокупность взаимодействующих компьютерных сетей масштаба предприятия, учреждения, организации.

27.Принципы планирования корпоративной сети учреждения культуры. Проектирование физической структуры корпоративной сети. Разработка логической структуры корпоративной сети. Проблемы оптимизации взаимодействия подсистем.

28.Понятие профиля пользователя. Основные виды: локальный, перемещаемый, постоянный.

29.Папки пользователя. Администрирование доступа к папкам и файлам.

30.Рабочие группы. Администрирование работы пользователей в рабочих группах.

31.Доменная структура корпоративной сети. Доменная система именования.

32.Служба ActiveDirectory и её структура: организационные единицы, домены, деревья, леса, сайты.

33.Безопасность при работе в сети. Средства обеспечения безопасности.

Примерные темы рефератов для контроля знаний

1. Логическая структуризация сети.
2. Линии связи и системы компьютерных сетей учреждений культуры и искусств.
3. Планирование рабочих групп и организация локальных компьютерных сетей в учреждениях культуры и искусств.
4. Обеспечение информационной безопасности в учреждениях культуры и искусств при сетевой работе.
5. Проектирование доменной структуры корпоративной сети учреждения, организации, предприятия.
6. Виртуальные локальные сети.
7. Цели и задачи администрирования компьютерных сетей учреждений культуры и искусств.

5. ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ

Учебная программа по дисциплине
«Администрирование компьютерных сетей»

Пояснительная записка

Современные компьютерные системы обработки информации функционируют в сетевом режиме. Этот режим обладает рядом особенностей, в частности, использование разделяемой коммуника-ционной среды, информационных ресурсов общего пользования, возможность использования объединенных вычислительных ресурсов и т.п. Пользователям становятся доступны многие сетевые сервисы. Все это требует серьезной подготовки каждого участника сетевого взаимодействия в области организации эффективной коллективной работы и обеспечения защиты информации.

Администрирование сетей предполагает достаточно глубокое знание и умение использовать все основные виды обеспечения сете-вых взаимодействий. В функции административной группы входит комплексное использование всех указанных видов обеспечения с учетом конкретных условий взаимодействия, архитектуры сети и уровня требований к безопасности и производительности.

Изучение учебной дисциплины имеет важное значение не только для специалистов, которые непосредственно заняты администрированием сетевой работы, но и конечных пользователей, для которых все более актуальной становится информация о возможных рисках и обеспечения безопасности работы в сети.

Содержанием учебной дисциплины предусмотрено формирование компетенций АК-1,4-9; САК 1-3,6,9; ПК 2-5,8-9 в соответствии с образовательнымстандартомвысшегообразованияпервойступенипоспециальности 1-21 04 01 «Культурология (понаправлениям».

Перечисленные компетенции предусматриваю формирование умений использования полученных знаний в теоретическом плане и при решении практических задач, умения самостоятельной работы, умения творчески решать практические задачи и предлагать нетривиальные решения, комплексно и системно использовать имеющиеся знания, обладать высокой информационной культурой, владеть навыками устной и письменной коммуникации, общения, бесконфликтного взаимодействия с участниками сетевого взаимодействия, умения разрешать ситуации межличностных взаимодействий, систематически и постоянно повышать квалификацию, владеть знаниями законов и права в предметной области, уметь реализовывать, прогнозировать и планировать свою деятельностьв сфере культуры и искусств, а также анализировать и правильно оценивать используемые сведения.

Целью изучения учебной дисциплины – является приобретение знаний, умений и навыков специалистом, участвующим в организации работ по автоматизации информационных процессов в учреждениях культуры и искусств.

Основными **задачами** учебной дисциплины являются:

– знакомство с базовыми принципами построения и эксплуатации компьютерных сетей уровня предприятия;

– изучение методов эффективной и безопасной работы в сетях различного уровня и комплексного их использования;

– приобретение навыков выполнения основных операций по управлению сетевым программным обеспечением и использованию средств защиты информации.

В результате изучения дисциплины обучаемый должен **знать:**

– цели и задачи администрирования корпоративных сетей;

– принципы организации сетевого взаимодействия в корпоративных системах;

– принципы действия сетевого оборудования и функционирования линий связи;

– сетевые возможности наиболее распостраненных операционных систем;

– основные принципы построения сетей масштаба предприятия, учреждения, организации и управления ими;

– методы адресации в локальных и глобальных сетях;

– основные принципы обеспечения информационной безопасности в сетях;

– методы и средства противодействия пассивным и активным методам нарушения информационной безопасности;

– организационно-правовые аспекты работы в сетевом режиме.

В результате изучения дисциплины обучаемый должен **уметь:**

– планировать логическую и физическую структуру локальных сетей для учреждений культуры и искусств;

– проектировать на концептуальном уровне локальные и корпоративные сети учреждений и организаций культуры;

– выполнять основные операции по организации сетевого взаимодействия в локальных и корпоративных сетях учреждений культуры;

– разрабатывать структуру управления безопасностью сети;

– выполнять основные настройки сетевого взаимодействия;

– выполнять основные операции по противодействию проникновениям и устранению угроз и последствий.

В результате изучения дисциплины студенты должны **владеть:**

– умениями инсталировать системное программное обеспечение;

– умениями создания одноранговых и доменных сетей;

– регистрацией пользователей и созданием перемещаемых профи-лей;

– знаниями о назначении прав доступа и обеспечения безопасного функционирования сети.

Изучение учебного материала связано с изучением учебных дисциплин «Компьютерная техника», «Основы информационных систем», «Основы информационнных технологий в культуре», Предусматривается знакомство с общими принципами построения вычислительных сетей, их физической и логической структурой, принципами передачи дискретных данных, аппаратным обеспечением локальных, корпоративных и глобальных сетей, линий связи,

принципами объединения сетей, изучение способов адресации и использования сетевых протоколов. Представляется важным практическое изучение организации сетевого взаимодействия в масштабе предприятия, организации, учреждения и, в частности, выполнение работ по установке необходимого ПО, настройке сетевого режима, установке необходимых сетевых служб, создание и настройка рабочих профилей пользователей, а также решения задач защиты сетей от атак и вторжений, как извне так и изнутри.

Учебным планом на изучение учебной дисциплины «Администрирование корпоративных сетей» всего предусмотрено 58 учебных часов, из них 28 часов аудиторные занятия. Аудиторные занятия включают 4 часа лекционных занятий и 24 часа лабораторных занятий. На управляемую самостоятельную работу предусмотрено 6 часов.

Рекомендуется преподавание учебной дисциплины на протяжении одного учебного семестра. В качестве формы итогового контроля предусмотрен зачет. Текущий контроль осуществляется при выполнении и сдаче лабораторных работ (проектов).

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Введение

Цель и задачи учебной дисциплины. Содержание и место учебной дисциплины в образовательном процессе. Основные формы и методы изучения дисциплины. Компетенции.

Тема 1. **Основы организации сетевого взаимодействия**

Понятие компьютерной сети, узла, линии и канала связи, сетевого оборудования.

Эволюция режимов работы компьютерных систем (монопольный, пакетный, разделения времени, сетевой).

Сетевой режим работы. Основные преимущества работы в сетевом режиме. Особенности работы в сети. Эволюция компьютерных сетей.

Основные требования к современным компьютерным сетям: доступность *(availability)*, отказоустойчивость *(faulttolerance)*, безопасность *(security)*, расширяемость *(extensibility)*, масштабируемость *(scalability)*, прозрачность *(transparency)*. Живучесть распределенных сетевых систем.

Сущность, цели и задачи администрирования компьютерных сетей. Стратегии администрирования. Распределения обязанностей по администрированию сложных корпоративных сетей.

Тема 2. **Сетевое взаимодействие компьютеров и устройств**

Взаимодействие компьютеров в сети. Понятие о технологии «клиент-сервер». Одноранговая и доменная организация сети.

Основные топологии физических связей при объединении нескольких компьютеров в сеть: полносвязная, магистральная, звезда, кольцо. Смешанные топологии и их использование при построении корпоративных сетей. Особенности функционирования.

Организация взаимодействия между устройствами в компьютерной сети. Понятие «открытая система». Модель взаимодействия открытых систем *(OpenSystemInterconnection, OSI*). Уровни *OSI*: прикладной, представительный, сеансовый, транспортный, сетевой, канальный, физический. Протоколы и интерфейсы.

Тема 3. **Стеки коммуникационных протоколов и адресация в сети**

Стандартные стеки коммуникационных протоколов: стек *TCP/IP (TransportControlProtocol/InternetProtocol*), стек *OSI*, стек *IPX/SPX (InternetworkPacketExchange/SequencedPacketExchange),* стек *NetBIOS/SMB (NetworkBasicInput/OutputSystem/ServerMessageBlock).*

Адресация компьютеров в сети. Цели и задачи адресации. Три схемы адресации узлов сети: физические, числовые и символьные адреса.

Аппаратные адреса. Назначение и структура *MAC*-адреса *(MediaAccessControl, MAC)*.

IP- и *IPX*-адреса. Классы *IP*-адресов (*версияIPv4*). Особые *IP*-адреса. Использование масок в *IP*-адресации. Распределение *IP*-адресов. Статические и динамические методы распределения *IP*-адресов.

Символьные имена узлов. Доменная система именования и ее структура.

Службы разрешения имен. Сервер *DNS (DomainNameSystem)*: назначение, принципы действия, организация. Централизованный и распределенный подходы к разрешению имен: особенности функционирования.

Реализация *NetBIOS*-имен. Служба *WINS*: назначение и применение.

Тема 4. **Компьютерные коммуникации и сетевое оборудование**

Линии связи и их классификация. Основные типы линий связи: проводные, кабельные (медные и оптоволоконные), наземная и спутниковая радиосвязь и их разновидности.

Технические характеристики линий связи: амплитудно-частотная, полоса пропускания и затухание. Пропускная способность линии. Помехоустойчивость и достоверность.

Кабельные линии связи. Кабели на основе неэкранированной витой пары *(UnshieldedTwistedPair, UTP)*. Кабели на основе экранированной витой пары *(ShieldedTwistedPair, STP)*. Назначение и применение. Коаксиальные кабели.

Оптоволоконные кабели: устройство, принципы действия, технические характеристики и применение в компьютерных сетях.

Передача сигналов по линиям связи. Аналоговая модуляция и цифровое кодирование. Методы аналоговой модуляции.

Цифровое кодирование. Основные способы дискретного кодирования данных. Методы обнаружения ошибок и компрессия данных. Применение избыточных кодов и скремблирования.

Методы коммутации абонентов. Сущность методов коммутации каналов на основе частотного мультиплексирования *(FrequencyDivisionMultiplexing, FDM)* и с разделением времени *(TimeDivisionMultiplexing, TDM)*.

Основные свойства сетей с коммутацией каналов. Принципы коммутации пакетов. Передача пакетов по виртуальным каналам. Динамические и статические виртуальные каналы.

Коммутация сообщений.

Технологии взаимодействия узлов в локальных сетях: *Ethernet, TokenRing, FDDI (FiberDistributedDataInterface)*. Общее описание технологии *Ethernet*: доступ к среде, возникновение, распознавание и разрешение коллизий. Пропускная способность сегмента *Ethernet.*

Средства технического обеспечения локальных сетей. Сетевые адаптеры: назначение, основные функции и технические характеристики. Повторители и концентраторы.

Коммутаторы и мосты. Принципы работы.

Логическая структуризация сети. Основные разновидности коммутаторов. Коммутация «на лету» и с буферизацией. Виртуальные локальные сети. Типовые схемы применения коммутаторов в локальных сетях.

Маршрутизация в глобальных сетях. Принципы действия маршрутизаторов. Шлюзы. Основные функции. Протоколы маршрутизации в *IP*-сетях. Коммутация и маршрутизация в корпоративных сетях.

Удалённый доступ. Выделенная линия, модемные соединения. Понятие модема и его основные функции.

Тема 5. **Проектирование корпоративной сети учреждений культуры**

Понятие корпоративной сети учреждения культуры. Цель и задачи создания корпоративной сети учреждения культуры как совокупности взаимодействующих сетей учреждений, предприятий, организаций и подразделений.

Проектирование физической структуры компьютерной сети. Разработка логической структуры. Оптимизация взаимодействия подсистем корпоративной сети.

Основные функциональные группы задач управления сетями. Управление конфигурацией сети и именованием. Выявление, определение и обработка ошибок. Анализ производительности и надёжности. Мониторинг и учет работы сети. Аудит.

Проектирование корпоративной сети на основе результатов системного анализа процессов управления учреждением культуры. Централизованные и распределённые системы управления корпоративными сетями. Построение систем управления крупными локальными и корпоративными сетями.

Тема 6. **Общие положения создания корпоративных сетей на платформе ОС Windows**

Эволюция сетевой поддержки операционными системами семейства *Windows.*

Файловая система *NTFS*. Основные возможности управления сетевым взаимодействием с помощью средств операционных систем семейства *Windows.*

Установка и первоначальная настройка серверной операционной системы *Windows*. Основные виды установки с диска (загрузка с установочного компакт-

диска, запуск из существующей операционной системы *Windows*, автоматические режимы установки с использованием файла ответов и клонирование серверной ОС с помощью*sysprep)*.

Роли сервера. Настройка основных ролей сервера.

Сервер DNS. Типы записей. Создание нового домена. Настройка сервера DNS.

Сервер *DHCP (DynamicHostConfigurationProtocol):* назначение, основные функции, принцип действия. Настройка сервера*DHCP*. Управление арендой адресов.

Подсистема ActiveDirectory. Концепция и определения ActiveDirectory.

Управление режимами домена.

Управление пользователями и группами. Структура записей пользователей и групп. Создание и редактирование учетных записей. Назначение паролей. Создание профилей пользователей (локальных, перемещаемых и обязательных).

Назначение разрешений и запрещений пользователям. Делегирование прав.

Управление компьютерами, принтерами и другими сетевыми устройствами.

Управление общими папками.

Подключение локальных и корпоративных сетей к сети Интернет. Система безопасности при доступе кИнтернет: межсетевой экран, противовирусная защита, устройство прокси-сервера, единая подсистема обеспечения безопасности пользователей. Авторизация пользователей.

Удалённый рабочий стол и удалённый помощник. *VPN*-соединения. Протоколы безопасного обмена:*IPSec, PPTP, L2TP*.

Основные принципы построения и управления сетью. Требования документирования топологии и устройств сети, IP-адресов хостов, каналов связи WAN, серверов и сегментов сети. Учет прав доступа и авторизация пользователей. Системный мониторинг производительности сети. Обоснованность развития и реконструкции. Оптимизация топологии. Минимизация административного трафика.

Основные методы подключения к Интернет. xDSL-соединение. Выделенная линия и её настройка. Виртуальная выделенная линия. Принципы создания VPN-соединения.

Тема 7. **Компьютерные сети на платформе WindowsServer**

Создание локальной сети на платформе WindowsServer 2003/2008/2012

Концепции групповой политики. Создание и назначение групповой политики.

Групповые политики при тонкой настройке сетевого взаимодействия. Основные компоненты объекта групповой политики: административные шаблоны, перенаправления папок, сценарии, параметры безопасности, политики прило-

жений. Кумулятивный и наследуемый характер групповых политик. Локальная и доменная групповые политики.

Установка и настройка Web-приложений. Службы IIS: Web-сервер, FTP-сервер, E-mail (серверы SMTP и POP3), служба новостей (NNTP-сервер). Установка и управление IIS.

Служба веб-публикаций. Виртуальные каталоги. Установка сайта. Размещение группы сайтов на одном сервере.

Подключение FTP-узлов. Создание и настройка сервера SMTP. Установка и настройка параметров POP3-сервера.

Виртуальные NNTP-серверы. Создание и настройка NNTP-сервера.

Защита IIS. Синхронизация работы сети

Создание и функционирование *интранет*как сети уровня предприятия. Основные службы *интранет*. Особенности организации работы. Структура *интранет*. Установка и настройка сервера приложений. Обеспечение безопасности в *интранет*.

Тема 8. **Создание корпоративных сетей на платформе операционной системы Linux**

Администрирование сетей на платформе Linux. Конфигурирование сетевых интерфейсов. Средства тестирования сети и сетевых настроек.

Установка и настройка *proxy*-сервера *Squid*. Настройка модемного соединения. Настройка связи с провайдером. Установка и настройка сетевых служб.

Установка и настройка *DHCP*. Установка и настройка *DHS*-сервера. Конфигурирование сетевой информационной службы*NIS.LDAP*-сервер. Настройка почтовых служб (серверы *SMTP*, *POP3, IMAP*). Установка, настройка и управление сервером *FTP*. Протокол *NNTP*. Настройка сервера новостей *INN*.

Web-сервер *Apache*.

Синхронизация работы сети.

Тема 9. **Практические и организационно-правовые аспекты организации безопасной работы в корпоративных сетях**

Содержание понятия «информационной безопасности корпоративных сетей». Риски проникновения. Виды нарушителей и выявление действий, направленных на подготовку атак.

Системный подход к обеспечению безопасности. Структура управления безопасностью сети. Понятие защищённости сети. Методы анализа защищённости.

Современные технологии защиты корпоративных сетей. Создание системы безопасности и обнаружения атак. Основные подсистемы обеспечения безопасности: межсетевые экраны, антивирусная защита, криптологические методы защиты.

Пассивные методы воздействия, основанные на прослушивании и анализе сетевого трафика. Противодействие прослушиванию сетевого трафика. Методы снижения риска преодоления парольной защиты.

Активные методы воздействия: сканирование уязвимостей, сетевые атаки, установка троянских программ, внедрение rootkits, заражение вирусами и сетевыми червями, взлом криптологической защиты, установка технических средств и бесконтактное считывание информации с устройств и линий коммуникации.

Обнаружение сканирования. Противодействие эксплойтам. Противодействие вирусам, сетевым червям и троянским программам. Обнаружение и устранение *rootkits*. Организация виртуальных ловушек.

Системы централизованного мониторинга безопасности. Противодействие проникновению с помощью дополнительных аппаратных средств.

Рекомендации по снижению угроз внешнего проникновения. Рекомендации по усилению защиты от внутренних нарушителей. Снижение рисков при несанкционированном доступе.

Срочные меры по ликвидации последствий проникновения. Устранение возможных угроз после проникновения.

Законодательные и нормативные документы о работе и безопасности в сети.

Авторское право. Проблемы соблюдения авторского права в сети.

Планирование систем безопасности в корпоративных сетях учреждений культуры и искусств.

Учебно-методическая карта учебнойдисциплины

дневная форма обучения

№№ тем	Темы	Количество аудиторных часов		Количество часов УСР	Форма контроля*
		лекции	лабораторные занятия		
1.	*Основы организации сетевого взаимодействия*	2		1	*фо*
2.	*Сетевое взаимодействие компьютеров и устройств*	2		1	*фо*
3.	*Стеки коммуникационных протоколов и адресация в сети*		2	1	*фо*
4.	*Компьютерные коммуникации и сетевое оборудование*		2	1	*нпо*
5.	*Проектирование корпоративной сети учреждений культуры*		2	1	*нпо*
6.	*Общие положения создания корпоративных сетей на платформе ОС Windows*		6		*по*
7.	*Компьютерные сети на платформе Windows-Server*		8		*по*
8.	*Создание корпоративных сетей на платформе операционной системы Linux*		2		*уо*
9.	*Практические и организационно-правовые аспекты организации безопасной работы в корпоративных сетях*		2	1	*уо*
	всего…	**4**	**24**	**4**	

1.	*Основы организации сетевого взаимодействия*	2		1	*фо*
2.	*Компьютерные коммуникации и сетевое оборудование*		2	1	*нпо*
3.	*Проектирование корпоративной сети учреждений культуры*		2		*нпо*
4.	*Общие положения создания корпоративных сетей на платформе ОС Windows*		2		*по*
5.	*Компьютерные сети на платформе Windows-Server*		2		*по*
	всего…	**2**	**8**	**2**	

- *фо* – фронтальный опрос, *уо* – устный опрос, *по* – письменный опрос.

ЛИТЕРАТУРА

Основная

1. Калинкина Т. И. Телекоммуникационные и вычислительные сети. Архитектура, стандарты и технологии: учебное пособие. – СПб.: БХВ-Петербург, 2010.

2. Кенин, А. М. Самоучитель системного администратора. – СПб.: БХВ-Петербург, 2012.

3. Моримото, Р. MicrosoftWindowsServer 2012: Полное руководство. Пер. с анг. /Рэнд Моримото, Майкл Ноэл, Гай Ярдени, Омар Драуби, Эндрю Аббейт, Крис Амарис. – М.: ООО «И.Д.Вильямс», 2013. – 1456 с.

Дополнительная

1. Колисниченко, Д.Н. Lunux-сервер своими руками / Д.Н.Колисниченко – СПб.: Наука и Техника, 2008. – 624 с.: ил.

2. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г.Олифер, Н.А.Олифер, – 4-е изд., перераб. и доп. – СПб.:Питер. – 2012. – 944 с.: ил.

3. Хассел, Дж. Администрирование WindowsServer 2003 / Дж. Хассел. – пер. с англ. – М.: Русская Редакция, СПб.: Питер, 2006. – 576 с.: ил.