МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине

«Информационно-коммуникационные технологии»

для направления подготовки 10.03.01 Информационная безопасность
направленность (профиль) Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Пятигорск 2023

ВВЕДЕНИЕ

1. Цель и задачи изучения дисциплины

Цель дисциплины: изучение принципов построения и основных топологий вычислительных сетей; ознакомление со способами и методами передачи информации в вычислительных сетях, с сервисными службами локальных и глобальных сетей; получение знаний о комплексировании сетей.

Задачи освоения дисциплины: ознакомление с принципами построения информационных сетей и телекоммуникаций; изучение модели взаимосвязи открытых систем, уровней и протоколов, топологии сетей, основные типы каналов связи, сети передачи данных; получение знаний об алгоритмах маршрутизации в сетях, сетевом программном обеспечении.

В результате освоения дисциплины студенты должны:

Знать:

- технологии поиска, хранения, обработки и анализа информации из различных источников и баз данных и представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий;
- современные компьютерные технологии работы с информацией в различных формах, использовать для ее получения, обработки, передачи, хранения и защиты;
- технологию инсталляции и настройки системного, прикладного и инструментального программного обеспечения систем автоматизации и управления;
- основы современных информационных технологий переработки и преобразования информации;
-современные технологии использования в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки.

Уметь:

- применять информацию и использовать для ее получения, обработки, передачи, хранения и защиты современные компьютерные технологии;
- использовать специальные документы в своей деятельности;
- осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять её в требуемом формате с использованием информационных, компьютерных и сетевых технологий;
- применять модели взаимосвязи открытых систем, уровней и протоколов, топологии сетей, основные типы каналов связи, сети передачи данных;

Владеть:

- принципами построения информационных сетей и телекоммуникаций;
- готовностью производить инсталляцию и настройку системного, прикладного и инструментального программного обеспечения систем автоматизации и управления;
- способностью использовать в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки;
- способностью использовать современные тенденции развития информационных технологий в профессиональной деятельности;
- специальными информационными и коммуникационными технологиями в будущей профессиональной деятельности.

2. Оборудование и материалы

Для проведения практических работ необходимо следующее материально-техническое обеспечение: персональный компьютер; проектор; возможность выхода в сеть Интернет для поиска по образовательным сайтам и порталам.

3. Наименование практических работ

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
4 семестр			
1	Практическая работа 1. Сеть, интерфейс, сервер, клиент, хост, терминал, протокол	1,5	
2	Практическая работа 2. ЛВС на основе технологий Ethernet	1,5	
3	Практическая работа 3. ЛВС на основе технологий Token Ring	1,5	
4	Практическая работа 4. ЛВС на основе технологий FDDI	1,5	
5	Практическая работа 5. Технологии передачи информации в компьютерных сетях Fast Ethernet.	1,5	
6	Практическая работа 6. Технологии передачи информации в компьютерных сетях Fiber Channel	1,5	
7	Практическая работа 7. Технологии передачи информации в компьютерных сетях ISDN.	1,5	
8	Практическая работа 8. Эталонная модель взаимосвязи открытых сетей (Модель OSI)	1,5	
9	Практическая работа 9. Объединение ЛВС. Корпоративные сети.	1,5	
10	Практическая работа 10. Территориально распределенные вычислительные сети. Принципы построения.	1,5	
11	Практическая работа 11. Разработка топологии иерархической сети	1,5	
12	Практическая работа 12. Маршрутизация в сетях	1,5	
13	Практическая работа 13. Сети с коммутацией каналов, пакетов, сообщений: ISDN, Frame Relay.	1,5	
14	Практическая работа 14. Беспроводные сети	1,5	
15	Практическая работа 15. Системы управления сетями, объекты и механизмы управления	1,5	
16	Практическая работа 16. Безопасность и защита данных.	1,5	
17	Практическая работа 17. Принципы построения Internet	1,5	
18	Практическая работа 18. Web-узлы.	1,5	
	Итого за 4 семестр	**27**	

Практическое занятие 1
Сеть, интерфейс, сервер, клиент, хост, терминал, протокол

Цель: дать студенту основные сведения о назначении и базовых понятиях ЛВС; основных классификационных признаках определения ЛВС

Теоретическая часть:

Лучшая ЛВС - это та, которая удовлетворяет всем требованиям пользователей, сформулированным в техническом задании на разработку ЛВС, при минимальном объеме капитальных и эксплуатационных затрат

Компьютерная сеть – это совокупность компьютеров, объединенных каналами передачи данных. В зависимости от расстояния между компьютерами различают следующие вычислительные сети:

- локальные вычислительные сети - LAN;
- территориальные вычислительные сети, к которым относятся региональные MAN и глобальные WAN сети;
- корпоративные сети.

Локальная сеть - это ЛВС, в которой ПК и коммуникационное оборудование находится на небольшом расстоянии друг от друга. ЛВС обычно предназначена для сбора, хранения, передачи, обработки и предоставления пользователям распределенной информации в пределах подразделения или фирмы. Кроме того, ЛВС, как правило, имеет выход в Интернет.

Локальные сети можно классифицировать по:

- уровню управления;
- назначению;
- однородности;
- административным отношениям между компьютерами;
- топологии;
- архитектуре.

Классификация ЛВС

По уровню управления выделяют следующие ЛВС:

- ЛВС рабочих групп, которые состоят из нескольких ПК, работающих под одной операционной системой. В такой ЛВС, как правило, имеется несколько выделенных серверов: файл-сервер, сервер печати;
- ЛВС структурных подразделений (отделов). ДанныеЛВС содержат несколько десятков ПК и серверы типа: файл-сервер, сервер печати, сервер баз данных;
- ЛВС предприятий (фирм). Эти ЛВС могут содержать свыше 100 компьютеров и серверы типа: файл-сервер, сервер печати, сервер баз данных, почтовый сервер и другие серверы.

По назначению сети подразделяются на:

- вычислительные сети, предназначенные для расчетных работ;
- информационно-вычислительные сети, которые предназначены, как для ведения расчетных работ, так и для предоставления информационных ресурсов;
- информационно-советующие, которые на основе обработки данных вырабатывают информацию для поддержки принятия решений;
- информационно-управляющие сети, которые предназначены для управления объектов на основе обработки информации.

По типам используемых компьютеров можно выделить:

- однородные сети, которые содержат однотипные компьютеры и системное программное обеспечение;
- неоднородные сети, которые содержат разнотипные компьютеры и системное программное.

По административным отношениям между компьютерами можно выделить:

- ЛВС с централизованным управлением (с выделенными серверами);
- ЛВС без централизованного управления (децентрализованные) или одноранговые (одноуровневые) сети.

По топологии (основным топологиям) ЛВС делятся на:

- топологию "шина";
- топологию "звезда";
- топологию "кольцо".

По архитектуре (основным типам архитектур) ЛВС делятся на:

1. Ethernet.
2. Arcnet.
3. Token ring.
4. FDDI.

Конфигурация ЛВС (локальные сети одноранговые и с выделенным сервером)

По административным отношениям между узлами можно выделить локальные сети с централизованным управлением или с выделенными серверами (серверные сети) и сети без централизованного управления или без выделенного сервера (децентрализованные), так называемые, одноранговые (одноуровневые) сети.

Локальные сети с централизованным управлением называются иерархическими, а децентрализованные локальные сети равноправными.

В локальных сетях с централизованным управлением один из компьютеров является сервером, а остальные ПК - рабочими станциями.

Серверы - это высокопроизводительные компьютеры с винчестерами большой емкости и с высокоскоростной сетевой картой, которые отвечают за хранение данных, организацию доступа к этим данным и передачу данных рабочим станциям или клиентам.

Рабочие станции. Компьютеры, с которых осуществляется доступ к информации на сервере, называются рабочими станциями или клиентами.

Одноранговые (одноуровневые или равноправные) локальные сети

В сетях с децентрализованным управлением нет единого центра управления взаимодействием рабочих станций и единого компьютера для хранения данных. Одноранговая локальная сеть – это ЛВС равноправных компьютеров, каждый из которых имеет уникальное имя и, как правило, пароль для входа в него в момент загрузки ОС.

Равноправность ПК означает, что администратор каждого компьютера в локальной сети может преобразовать свой локальный ресурс в разделяемый и устанавливать права доступа к нему и пароли. Он же отвечает за сохранность или работоспособность этого ресурса. Локальный ресурс - ресурс, доступный только с ПК, на котором он находится. Ресурс ПК, доступный для других компьютеров, называется разделяемым или совместно используемым.

Таким образом, одноранговая локальная сеть - это ЛВС, в которой каждая рабочая станция может разделить все или некоторые из ее ресурсов с другими рабочими станциями сети.

Но отсутствие выделенного сервера не позволяет администратору централизовано управлять всеми ресурсами одноранговой локальной сети.

Каждая рабочая станция может выполнять функции, как клиента, так и сервера, т.е. предоставлять ресурсы другим рабочим станциям и использовать ресурсы других рабочих станций. .

Серверные локальные сети (многоуровневые или иерархические)

В локальных сетях с централизованным управлением сервер обеспечивает взаимодействия между рабочими станциями, выполняет функции хранения данных общего пользования, организует доступ к этим данным и передает данные клиенту. Клиент обрабатывает полученные данные и предоставляет результаты обработки пользователю. Необходимо отметить, что обработка данных может осуществляться и на сервере.

Локальные сети с централизованным управлением, в которых сервер предназначен только хранения и выдачи клиентам информации по запросам, называются сетями с выделенным файл-сервером. Системы, в которых на сервере наряду с хранением осуществляется и обработка информации, называются системами "клиент-сервер".

Необходимо отметить, что в серверных локальных сетях клиенту непосредственно Программное обеспечение, управляющее работой ЛВС с централизованным управлением, состоит из двух частей:

- сетевой операционной системы, устанавливаемой на сервере;
- программного обеспечения на рабочей станции, представляющего набор программ, работающих под управлением операционной системы, которая установлена на рабочей станции. При этом на разных рабочих станциях в одной сети могут быть установлены различные операционные системы.

В больших иерархических локальных сетях в качестве сетевых ОС используются UNIX и LINUX, которые являются более надежными. Для локальных сетей среднего масштаба наиболее популярной сетевой ОС является Windows 2003 Server.

В зависимости от способов использования сервера в иерархических сетях различают серверы следующих типов:

1. Файловый сервер. В этом случае на сервере находятся совместно обрабатываемые файлы или (и) совместно используемые программы.
2. Сервер баз данных. На сервере размещается сетевая база данных.
3. Принт-сервер. К компьютеру подключается достаточно производительный принтер, на котором может быть распечатана информация сразу с нескольких рабочих станций.
4. Почтовый сервер. На сервере хранится информация, отправляемая и получаемая как по локальной сети.

Достоинства:

- выше скорость обработки данных;
- обладает надежной системой защиты информации и обеспечения секретности;
- проще в управлении по сравнению с одноранговыми сетями.

Недостатки:

- сеть дороже из-за выделенного сервера;
- менее гибкая по сравнению с равноправной сетью.

Контрольные вопросы

1. Объясните разницу между централизованной и распределенной обработкой информации
2. Общие ресурсы вычислительных сетей
3. Централизованная и распределенная обработка информации
4. Сервисы в сетях.

Практическое занятие 2
ЛВС на основе технологий Ethernet

Цель: ознакомить студентов с современными топологиями построения сетей, сравнительными характеристиками топологий, определять в каких сетях, эффективнее использовать ту или иную топологию.

Теоретическая часть:

В зависимости от топологии различают сети: шинной, кольцевой, звездной, иерархической и произвольной структуры.

Различают физическую и логическую топологию. Логическая и физическая топологии сети независимы друг от друга. Физическая топология - это геометрия

построения сети, а логическая топология определяет направления потоков данных между узлами сети и способы передачи данных.

В настоящее время в локальных сетях используются следующие физические топологии:

- физическая "шина" (bus);
- физическая “звезда” (star);
- физическое “кольцо” (ring);
- физическая "звезда" и логическое "кольцо" (Token Ring).

Шинная топология

Сети с шинной топологией (Рисунок 1) используют линейный моноканал (коаксиальный кабель) передачи данных, на концах которого устанавливаются оконечные сопротивления (терминаторы). Каждый компьютер подключается к коаксиальному кабелю с помощью Т-разъема (Т - коннектор). Данные от передающего узла сети передаются по шине в обе стороны, отражаясь от оконечных терминаторов. Терминаторы предотвращают отражение сигналов, т.е. используются для гашения сигналов, которые достигают концов канала передачи данных.

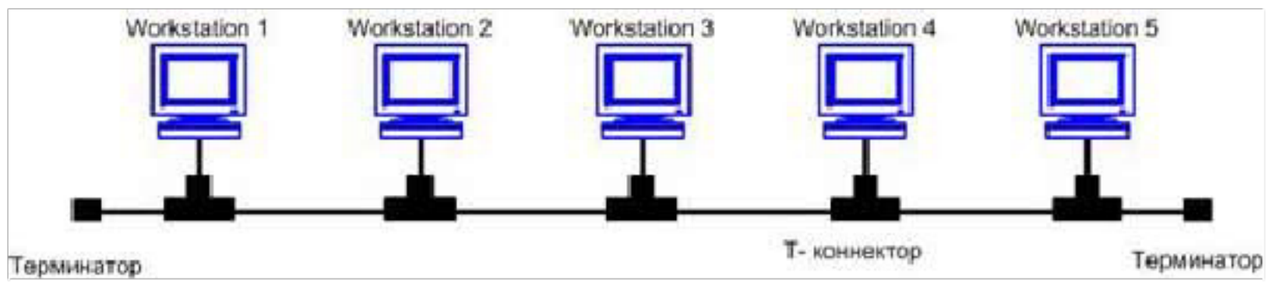


Рисунок 1 – Шинная топология

Таким образом, информация поступает на все узлы, но принимается только тем узлом, которому она предназначается. В топологии логическая шина среда передачи данных используются совместно и одновременно всеми ПК сети, а сигналы от ПК распространяются одновременно во все направления по среде передачи. Так как передача сигналов в топологии физическая шина является широковещательной, т.е. сигналы распространяются одновременно во все направления, то логическая топология данной локальной сети является логической шиной.

Данная топология применяется в локальных сетях с архитектурой Ethernet (классы 10Base-5 и 10Base-2 для толстого и тонкого коаксиального кабеля соответственно).

Преимущества сетей шинной топологии:

- отказ одного из узлов не влияет на работу сети в целом;
- сеть легко настраивать и конфигурировать;
- сеть устойчива к неисправностям отдельных узлов.

Недостатки сетей шинной топологии:

- разрыв кабеля может повлиять на работу всей сети;
- ограниченная длина кабеля и количество рабочих станций;
- трудно определить дефекты соединений.

Топология типа “звезда”

В сети, построенной по топологии типа “звезда” (Рисунок 2) каждая рабочая станция подсоединяется кабелем (витой парой) к концентратору или хабу (*hub*). Концентратор обеспечивает параллельное соединение ПК и, таким образом, все компьютеры, подключенные к сети, могут общаться друг с другом.

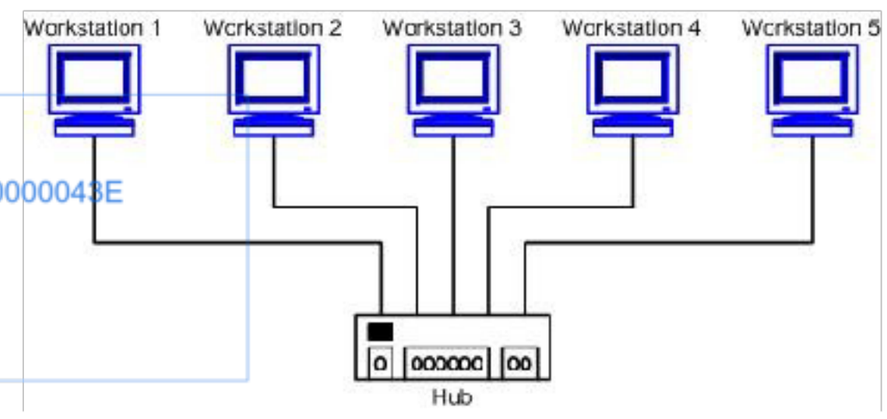


Рисунок 2 – Радиальная топология типа «звезда»

Данные от передающей станции сети передаются через хаб по всем линиям связи всем ПК. Информация поступает на все рабочие станции, но принимается только теми станциями, которым она предназначается. Так как передача сигналов в топологии физическая звезда является широковещательной, т.е. сигналы от ПК распространяются одновременно во все направления, то логическая топология данной локальной сети является логической шиной.

Данная топология применяется в локальных сетях с архитектурой 10Base-T Ethernet.

Преимущества сетей топологии звезда:

- легко подключить новый ПК;
- имеется возможность централизованного управления;
- сеть устойчива к неисправностям отдельных ПК и к разрывам соединения отдельных ПК.

Недостатки сетей топологии звезда:

- отказ хаба влияет на работу всей сети;
- большой расход кабеля.

Топология “кольцо”

В сети с топологией кольцо все узлы соединены каналами связи в неразрывное кольцо (необязательно окружность), по которому передаются данные. Выход одного ПК соединяется со входом другого ПК. Начав движение из одной точки, данные, в конечном счете, попадают на его начало. Данные в кольце всегда движутся в одном и том же направлении. Принимающая рабочая станция распознает и получает только адресованное ей сообщение. В сети с топологией типа физическое кольцо используется маркерный доступ, который предоставляет станции право на использование кольца в определенном порядке. Логическая топология данной сети - логическое кольцо. Данную сеть очень легко создавать и настраивать.

К основному недостатку сетей топологии кольцо является то, что повреждение линии связи в одном месте или отказ ПК приводит к неработоспособности всей сети.

Как правило, в чистом виде топология “кольцо” не применяется из-за своей ненадёжности, поэтому на практике применяются различные модификации кольцевой топологии.

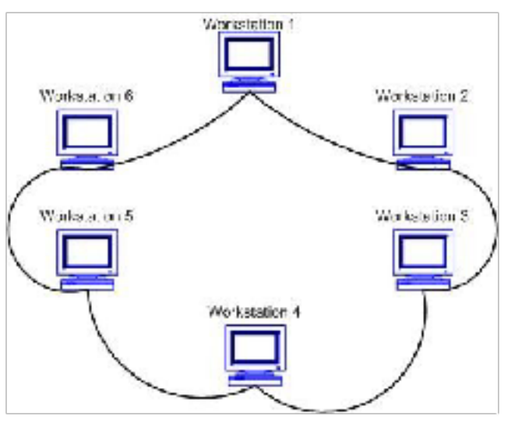


Рисунок 3 – Топология “кольцо”

Контрольные вопросы:

1. Типы топологии сетей, схемы, принцип действия.
2. Сравнительные характеристики базовых топологий
3. Преимущества и недостатки технологии топология Ethernet

Практическое занятие 3
ЛВС на основе технологий Token Ring

Цель: ознакомить студентов с современными топологиями построения сетей, сравнительными характеристиками топологий, определять в каких сетях, эффективнее использовать ту или иную топологию.

В архитектуре Token Ring маркер передаётся от узла к узлу по логическому кольцу, созданному центральным концентратором. Такая маркерная передача осуществляется в фиксированном направлении (направление движения маркера и пакетов данных представлено на рисунке стрелками синего цвета). Станция, обладающая маркером, может отправить данные другой станции.

Для передачи данных рабочие станции должны сначала дождаться прихода свободного маркера. В маркере содержится адрес станции, пославшей этот маркер, а также адрес той станции, которой он предназначается. После этого отправитель передает маркер следующей в сети станции для того, чтобы и та могла отправить свои данные.

Один из узлов сети (обычно для этого используется файл-сервер) создаёт маркер, который отправляется в кольцо сети. Такой узел выступает в качестве активного монитора, который следит за тем, чтобы маркер не был утерян или разрушен.

Преимущества сетей топологии Token Ring:

- топология обеспечивает равный доступ ко всем рабочим станциям;
- высокая надежность, так как сеть устойчива к неисправностям отдельных станций и к разрывам соединения отдельных станций.

Недостатки сетей топологии Token Ring: большой расход кабеля и соответственно дорогостоящая разводка линий связи.

Топология Token Ring основана на топологии "физическое кольцо с подключением типа звезда" (Рисунок 4). В данной топологии все рабочие станции подключаются к центральному концентратору (Token Ring) как в топологии физическая звезда. Центральный концентратор - это интеллектуальное устройство, которое с помощью перемычек обеспечивает последовательное соединение выхода одной станции с входом другой станции.

Другими словами с помощью концентратора каждая станция соединяется только с двумя другими станциями (предыдущей и последующей станциями). Таким образом, рабочие станции связаны петлей кабеля, по которой пакеты данных передаются от одной станции к другой и каждая станция ретранслирует эти посланные пакеты. В каждой рабочей станции имеется для этого приемо-передающее устройство, которое позволяет управлять прохождением данных в сети. Физически такая сеть построена по типу топологии “звезда”.

Концентратор создаёт первичное (основное) и резервное кольца. Если в основном кольце произойдёт обрыв, то его можно обойти, воспользовавшись резервным кольцом, так как используется четырёхжильный кабель. Отказ станции или обрыв линии связи рабочей станции не влечет за собой отказ сети как в топологии кольцо, потому что концентратор отключает неисправную станцию и замкнет кольцо передачи данных.

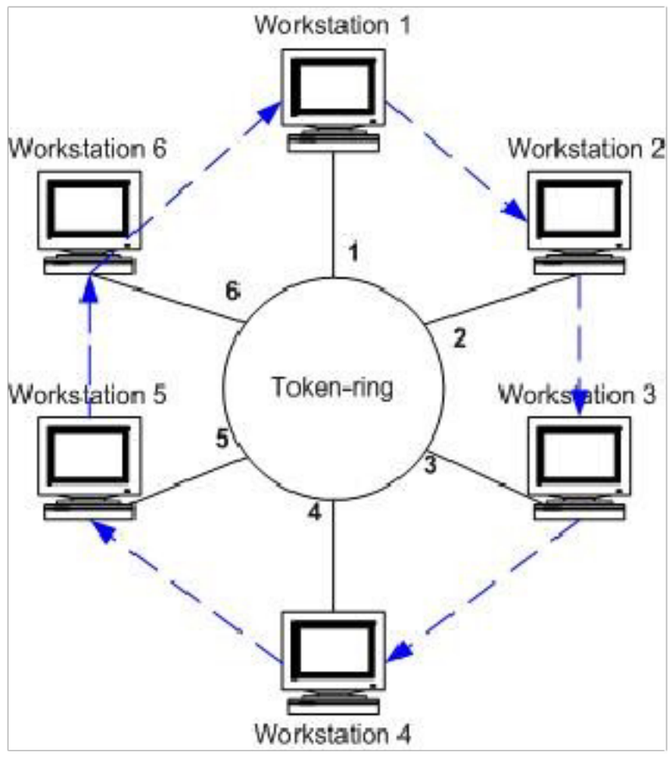


Рисунок 4 – Топология Token Ring

Контрольные вопросы:

4. Типы топологии сетей, схемы, принцип действия.
5. Сравнительные характеристики базовых топологий
6. Объясните разницу, между топологиями “кольцо”
7. Преимущества и недостатки технологии топология Token Ring

Практическое занятие 4
ЛВС на основе технологий FDDI

Цель: ознакомить студентов с современными топологиями построения сетей, сравнительными характеристиками топологий, определять в каких сетях, эффективнее использовать ту или иную топологию.

Технология FDDI предназначена не для непосредственного соединения компьютеров, а для построения высокоскоростных магистральных каналов связи (backbone), объединяющих несколько сегментов локальной сети. Простейшим примером такой магистрали являются два сервера, соединенные высокоскоростным каналом связи, созданным на базе двух сетевых карт и кабеля. Так же, как и технология 100Base-T, FDDI обеспечивает скорость передачи данных 100 Мбит/с.

Технология FDDI (Fiber Distributed Data Interface) – оптоволоконный интерфейс распределенных данных - это первая технология локальных сетей, в которой средой передачи данных является волоконно-оптический кабель. Технология FDDI появилась в середине 80-х годов.

Технология FDDI во многом основывается на технологии Token Ring, поддерживая метод доступа с передачей маркера.

Сеть FDDI использует топологию двойного физического кольца (двух оптоволоконных колец), которые образуют основной и резервный путь передачи данных между узлами сети. Наличие двух колец – это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят воспользоваться этим повышенным потенциалом надежности, должны быть подключены к обоим кольцам.

Передающиеся сигналы движутся по кольцам в противоположных направлениях. Одно из колец называется первичным, а другое - вторичным. При корректном функционировании сети первичное кольцо используется для передачи данных, а вторичное выступает в роли запасного.

В сети FDDI каждое сетевое устройство (узел сети) играет роль повторителя. FDDI поддерживает четыре вида узлов: станция с двойным подключением (DAS - dual-attached stations), станция с одинарным подключением (SAS - single-attached stations),

концентратор с двойным подключением (DAC - dual-attached concentrator) и концентратор с одинарным подключением (SAC-single-attached concentrator). DAS и DAC всегда подключаются к обоим кольцам, а SAS и SAC - только к первичному кольцу.

Если в какой-либо точке сети возникает разрыв кабеля или другая поломка, делающая невозможной передачу данных между соседними узлами сети, то устройства DAS и DAC восстанавливают работоспособность сети, перенаправляя сигнал в обход неработоспособного сегмента с использованием вторичного кольца.

FDDI использует маркер доступа в качестве протокола контроля доступа к среде передачи и оптический кабель в качестве среды передачи.

В нормальном режиме работы сети данные проходят через все узлы и все участки кабеля только первичного (Primary) кольца, этот режим назван режимом Thru - «сквозным», или «транзитным». Вторичное кольцо (Secondary) в этом режиме не используется.

В случае какого-либо вида отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), первичное кольцо объединяется с вторичным, вновь образуя единое кольцо (Рис. 5). Этот режим работы сети называется Wrap, то есть, «свертывание» или «сворачивание» колец. Операция свертывания производится средствами концентраторов и/или сетевых адаптеров FDDI. Для упрощения этой процедуры, данные по первичному кольцу, всегда передаются в одном направлении (на диаграммах это направление изображается против часовой стрелки), а по вторичному – в обратном (изображается по часовой стрелке). Поэтому при образовании общего кольца из двух колец передатчики станций по-прежнему остаются подключенными к приемникам соседних станций, что позволяет правильно передавать и принимать информацию соседними станциями.

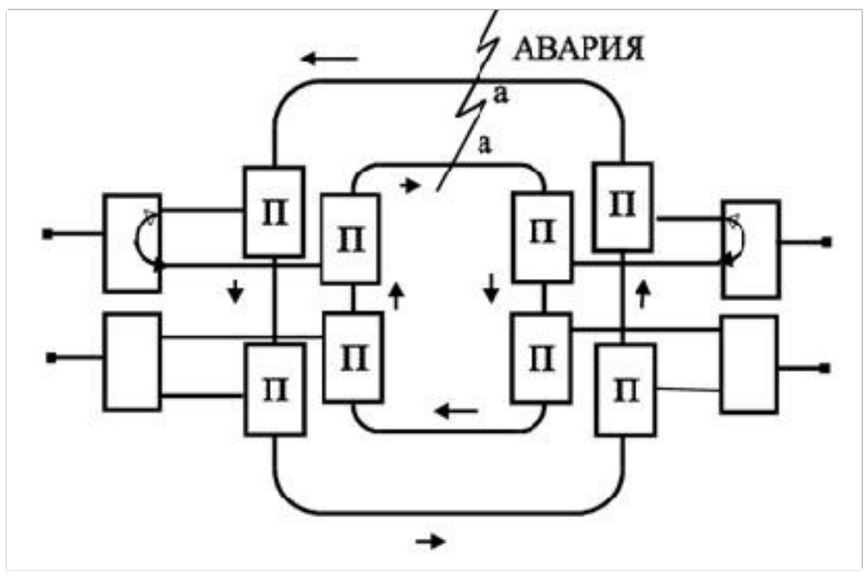


Рисунок 5 - ИВС с двумя циклическими кольцами в аварийном режиме

Сеть FDDI может полностью восстанавливать свою работоспособность в случае единичных отказов ее элементов. При множественных отказах сеть распадается на несколько не связанных сетей.

Кольца в сетях FDDI рассматриваются как общая разделяемая среда передачи данных, поэтому для нее определен специальный метод доступа. Этот метод очень близок к методу доступа сетей Token Ring и также называется методом маркерного (или токенного) кольца – token ring.

Отличия метода доступа заключаются в том, что время удержания маркера в сети FDDI не является постоянной величиной. Это время зависит от загрузки кольца - при небольшой загрузке оно увеличивается, а при больших перегрузках может уменьшаться до нуля. Эти изменения в методе доступа касаются только асинхронного трафика, который не критичен к небольшим задержкам передачи кадров. Для синхронного трафика время удержания маркера по-прежнему остается фиксированной величиной.

Технология FDDI в настоящее время поддерживает типа кабелей:

– волоконно-оптический кабель;

– неэкранированная витая пара категории 5. Последний стандарт появился позже оптического и носит название TP-PMD (Physical Media Dependent).

Оптоволоконная технология обеспечивает необходимые средства для передачи данных от одной станции к другой по оптическому волокну и определяет:

• использование в качестве основной физической среды многомодового волоконно-оптического кабеля 62,5/125 мкм;

• требования к мощности оптических сигналов и максимальному затуханию между узлами сети. Для стандартного многомодового кабеля эти требования приводят к предельному расстоянию между узлами в 2 км, а для одномодового кабеля расстояние увеличивается до 10–40 км в зависимости от качества кабеля;

• требования к оптическим обходным переключателям (optical bypass switches) и оптическим приемопередатчикам;

• параметры оптических разъемов MIC (Media Interface Connector), их маркировку;

• использование для передачи света с длиной волны в 1,3 нм;

Максимальная общая длина кольца FDDI составляет 100 километров, максимальное число станций с двойным подключением в кольце - 500.

Технология FDDI разрабатывалась для применения в ответственных участках сетей - на магистральных соединениях между крупными сетями, например сетями зданий, а также для подключения к сети высокопроизводительных серверов. Поэтому главные требования, у разработчиков были (достоинства):

- обеспечение высокой скорости передачи данных,
- отказоустойчивость на уровне протокола;
- большие расстояния между узлами сети и большое количество подключенных станций.

Все эти цели были достигнуты. В результате технология FDDI получилась качественной, но весьма дорогой (недостаток). Даже появление более дешевого варианта для витой пары, не намного снизило стоимость подключения одного узла к сети FDDI. Поэтому практика показала, что основной областью применения технологии FDDI стали магистрали сетей, состоящих из нескольких зданий, а также сети масштаба крупного города, то есть класса MAN.

Технология FDDI имеет следующие преимущества.

Топология двойного физического кольца обеспечивает надежность передачи данных путем сохранения работоспособности сети в случае обрыва кабеля. В стандарт FDDI заложены функции управления сетью. В дополнение к перечисленным преимуществам существует спецификация (CDDI - Copper Distributed Data Interface) на построение сети по технологии FDDI с использованием медной витой пары. Эта спецификация позволяет снизить стоимость развертывания сети за счет использования менее дорогого медного кабеля вместо оптического.

Основным недостатком FDDI является цена построения сети. Сетевые карты и оптический кабель для FDDI обладают существенно большей стоимостью, чем для других технологий, обеспечивающих такую же скорость передачи данных. Специфика монтажа оптического кабеля требует дополнительной подготовки специалистов, выполняющих работу с кабелем. Несмотря на то, что сетевые карты CDDI дешевле FDDI, тем не менее они являются более дорогими, чем сетевые карты 100Base-T.

Контрольные вопросы:

1.Типы топологии сетей, схемы, принцип действия.

2. Сравнительные характеристики базовых топологий

3. Характеристики Технологии FDD.

4. Преимущества и недостатки технологии FDDI

5. Схема ИВС с двумя циклическими кольцами

6. Функции Технологии FDDI

Практическое занятие 5
Технологии передачи информации в компьютерных сетях Fast Ethernet.

Цель: дать студенту основные сведения о существующих технологиях передачи информации в компьютерных сетях.

Теоретическая часть:

Существуют следующие технологии передачи информации в компьютерных сетях: Fast Ethernet, IEEE 1394/USB, Fiber Channel, FDDI, X.25, Frame Relay, ATM, ISDN, ADSL, SONET. Первые четыре технологии передачи данных: Fast Ethernet, IEEE 1394/ USB, Fiber Channel и FDDI относят к технологиям локальных сетей. Оставшиеся создавались для глобальных каналов связи. Рассмотрим некоторые из распространенных технологий передачи данных - Fast Ethernet, Fiber Channel, FDDI, ISDN.

Fast Ethernet или «**100Base-T**» - это высокоскоростная технология передачи данных в локальных сетях. Правила передачи данных с использованием этой технологии определяются стандартом IEEE 802.3u. Этот стандарт описывает правила работы протоколов второго уровня модели OSI (канальный уровень) и предоставляет возможность передачи данных со скоростью 100 Мбит/с.

Технология 100Base-T - это высокоскоростная технология передачи данных в локальных сетях. Правила передачи данных с использованием этой технологии определяются стандартом IEEE 802.3u. Этот стандарт описывает правила работы протоколов второго уровня модели OSI (канальный уровень) и предоставляет возможность передачи данных со скоростью 100 Мбит/с.

Технология 100Base-T использует метод CSMA/CD в качестве протокола контроля доступа к среде передачи. 100Base-T базируется на возможностях масштабирования, обеспечиваемых методом CSMA/CD. Масштабирование подразумевает возможность простого увеличения или уменьшения размеров сети без значительного снижения ее производительности, надежности и управляемости. Технология 100Base-T использует кабель UTP5 (неэкранированная витая пара 5-й категории).

Технология 100Base-T имеет следующие особенности.

1. В связи с применением одинакового протокола контроля доступа к среде передачи - CSMA/CD сети, использующие технологию 10Base-T Ethernet, легко переводятся на более высокоскоростную технологию 100Base-T. Поэтому многие производители выпускают сетевые карты, поддерживающие обе технологии передачи данных: 10Base-T Ethernet и 100Base-T. Такие сетевые карты имеют встроенные возможности автоматического определения скорости передачи данных в сети и автоматической настройки на соответствующий режим работы. Поскольку технологии 10Base-T Ethernet и 100Base-T могут легко сосуществовать в одной сети, администраторы получают очень высокую степень гибкости по переводу станций с технологии 10Base-TEthernet на 100Base-T.
2. Кабель UTP5 и сетевые карты 100Base-T в настоящее время выпускаются огромным количеством производителей.

Недостаткам использования технологии 100Base-T являются существенно большие ограничения на длину кабельных сегментов, чем в технологии 10Base-T Ethernet. По сравнению с технологией 10Base-T Ethernet, позволяющей организовывать сети максимального диаметра размером 500 м, технология 100Base-T ограничивает этот диаметр 205 м. Для существующих сетей, превышающих этот лимит, потребуется установка дополнительных маршрутизаторов.

Перспективность использования технологии 10Base-T заключается в том, что новая технология Gigabit Ethernet (также известная как 1000Base-T или IEEE 802.3z) разрабатывается с учетом возможности использования существующих кабельных систем на базе UTP5. При этой технологии скорость передачи данных в сети увеличивается до 1000 Мбит/с, что в десять раз быстрее передачи данных по технологии 100Base-T.

Контрольные вопросы:

1.Краткая характеристика технологии передачи информации Ethernet?

2.Преимущества и недостатки данной технологии.

Практическое занятие 6
Технологии передачи информации в компьютерных сетях Fiber Channel

Цель: дать студенту основные сведения о существующих технологиях передачи информации в компьютерных сетях.

Теоретическая часть:

Технологии построения сети сводятся к тому, чтобы связать между собой удаленные устройства электрически и информационно, то есть, создать физическую среду передачи (кабель, беспроводная связь) и обеспечить общий протокол передачи данных по сети.

Одной из относительно новых технологий передачи данных является Fiber Channel.

Технология **Fiber Channel** основывается на применении оптического волокна в качестве среды передачи данных. Наиболее часто встречающимся применением этой технологии в настоящее время являются высокоскоростные сетевые устройства хранения данных (SAN - Storage Area Networks). Такие устройства используются для построения высокопроизводительных кластерных систем. Технология Fiber Channel изначально создавалась как интерфейс, обеспечивающий возможность высокоскоростного обмена данными между жесткими дисками и процессором компьютера. Позже стандарт был дополнен и сейчас определяет механизмы взаимодействия не только систем хранения данных, но и способов взаимодействия нескольких узлов кластерной системы между собой и средствами хранения данных.

Технология Fiber Channel опирается на использование нескольких видов специализированного оборудования: оптический кабель, специализированные коммутаторы и преобразователи (Gigabit Interface Converter - GBIC). GBIC используются для преобразования электрического сигнала в световой и обратно. Стандартом поддерживаются два типа оптических кабелей: одноволновой (single-mode) и многоволновой (multimode). Многоволновой кабель имеет больший диаметр и позволяет передачу одновременно нескольких световых волн. Одноволновой кабель обеспечивает наличие единственной световой волны при передаче данных. Наличие нескольких волн (полезная и несколько паразитных) в кабеле ухудшает характеристики среды передачи и, как следствие, многоволновой кабель позволяет передавать данные без повторителей на расстояния примерно в 10 раз меньшие, чем одноволновой.

Технология Fiber Channel имеет несколько преимуществ по сравнению с другими средами передачи данных, важнейшим из которых является скорость.

Вторым важным преимуществом является возможность передачи сигнала на очень большие расстояния. Обмен данными с использованием светового сигнала вместо электрического обеспечивает возможность передачи информации на расстояния до 10-20 км без использования повторителей (при применении одноволнового кабеля).

Третьим преимуществом технологии Fiber Channel является полный иммунитет к электромагнитным помехам. Это качество позволяет активно использовать оптическую среду передачи даже в производственных помещениях с большим количеством электромагнитных помех. Четвертое преимущество состоит в полном отсутствии излучения сигнала в окружающую среду, что дает возможность применения Fiber Channel в сетях с повышенными требованиями к безопасности обрабатываемых и хранимых данных.

Основным недостатком технологии Fiber Channel является ее стоимость: оптический кабель со всеми сопутствующими его использованию разъемами и способами монтажа является существенно более дорогим, чем медные кабели.

Для организации высокоскоростных локальных сетей используется FDDI, рассмотрена выше (Fiber Distributed Data Interface).

Контрольные вопросы:

1. Характеристика технологии передачи информации Fiber Channel.
2. Преимущества и недостатки данной технологии.

Практическое занятие 7
Технологии передачи информации в компьютерных сетях ISDN.

Цель: дать студенту основные сведения о существующих технологиях передачи информации в компьютерных сетях.

Теоретическая часть:

Технология обмена цифровыми данными с использованием телефонных линий **Integrated Services Digital Network (ISDN)** предоставляет возможность обмена данными в виде передачи цифровых сигналов по цифровым телефонным линиям. Эти данные могут представлять собой комбинацию видео, звуковых и других данных. ISDN имеет несколько технологических решений, обеспечивающих заказчика необходимой производительностью канала связи. Для частных лиц и небольших офисов в основном предоставляются линии с базовой скоростью (Basic Rate Interface - BRI). Для крупных компаний предоставляются линии Primary Rate Interface - PRI. BRI использует два «несущих» (bearer - B) канала связи с пропускной способностью 64 Кбит/с каждый для приема и передачи данных и один управляющий канал (delta - D) для установки и поддержания соединения. PRI - это совокупность нескольких цифровых линий, используемых параллельно для приема и передачи данных. Такие совокупности линий получили условные обозначения T1 и E1. В США стандартом является применение линий Tl. T1 состоит из 23 B-каналов и одного D-канала с суммарной пропускной способностью 1,544 Мбит/с.

В Европе используются линии E1. E1 состоит из 30 B-каналов и одного D-канала с суммарной пропускной способностью 2,048 Мбит/с.

ISDN требует применения специального оборудования, включающего в себя цифровые телефонные линии, и преобразователей (network termination unit - NT-1). NT-1 преобразует входной сигнал в цифровой, равномерно распределяет его по каналам для передачи и выполняет диагностический анализ состояния всей линии передачи данных. NT-1 является и точкой подключения к цифровой сети различного оборудования: телефонов, компьютеров и т.п. Также NT-1 может выполнять функции преобразователя для подключения оборудования, самостоятельно не поддерживающего ISDN.

Преимущества ISDN заключаются в следующем.

1. Увеличена скорость обмена данными с дополнительными возможностями интеграции данных, голоса и видео в единый поток.
2. С использованием ISDN вы имеете возможность передавать данные и голосовой трафик одновременно по одной телефонной линии.

К недостатку ISDN относится медленное распространение в связи с необходимостью преобразования существующей инфраструктуры телефонных сетей, что неминуемо влечет существенные затраты.

Контрольные вопросы

1. Характеристика технологии передачи информации ISDN.

2. Преимущества, недостатки.

Практическое занятие 8
Эталонная модель взаимосвязи открытых сетей (Модель OSI)

Цель: дать студенту основные сведения о семиуровневой эталонной модели взаимодействия открытых систем – OSI, схему взаимодействия по уровням модели OSI, понятия: протокол, интерфейс, стек протоколов; описать функции каждого из уровней модели OSI.

Теоретическая часть:

Многоуровневое представление средств сетевого взаимодействия позволяет выбирать структуру и средства реализации проектируемой ЛВС.

Для обеспечения нормального взаимодействия оборудования в сетях необходим единый унифицированный стандарт, который определял бы алгоритм передачи информации в сетях. В современных вычислительных сетях роль такого стандарта выполняют сетевые протоколы.

Сетевая модель - это модель взаимодействия сетевых протоколов. Сетевым протоколом называется набор правил, позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть компьютерами.

В связи с тем, что описать единым протоколом взаимодействия между устройствами в сети не представляется возможным, то необходимо разделить процесс сетевого взаимодействия на ряд концептуальных уровней (модулей) и определить функции для каждого модуля и порядок их взаимодействия, применив метод декомпозиции.

Используется многоуровневый подход метода декомпозиции, в соответствии с которым множество модулей решающих частные задачи упорядочивают по уровням образующим иерархию, процесс сетевого взаимодействия можем представить в виде иерархически организованного множества модулей.

Протокол, интерфейс, стек протоколов

Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют две стороны, то есть необходимо организовать согласованную работу двух иерархий, работающих на разных компьютерах (рис. 6).

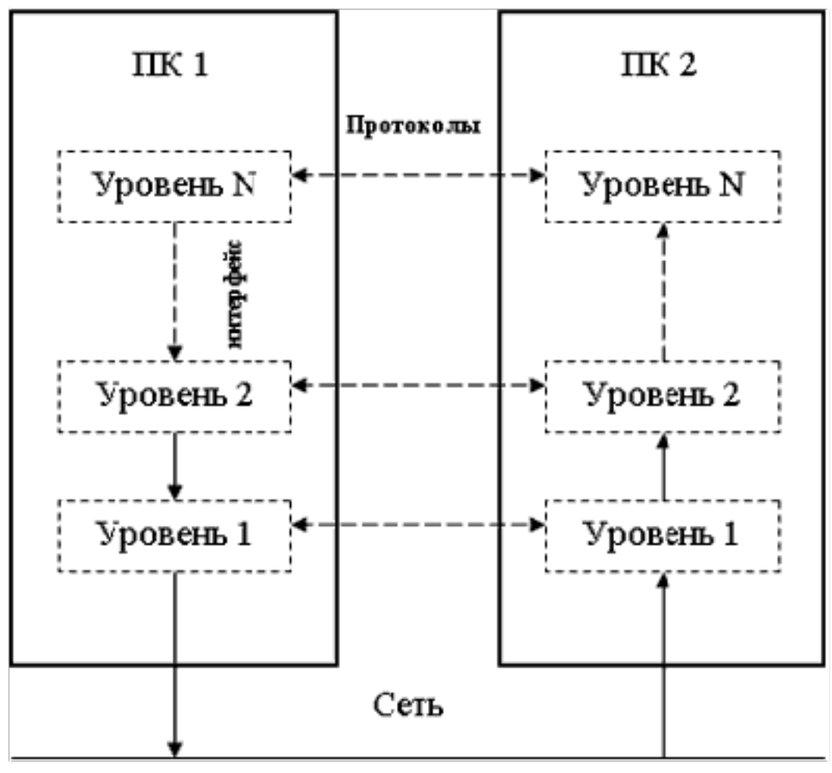


Рисунок 6 – Многоуровневое представление средств сетевого взаимодействия

Семиуровневая эталонная модель OSI. Модель OSI-ISO

Эталонная модель OSI (Open System Interconnection - OSI), разработанная в 1984 году Международной организацией по стандартизации (International Organization of

Standardization – ISO), является определяющим документом концепции разработки открытых стандартов для организации соединения систем. Открытая система - система, доступная для взаимодействия с другими системами в соответствии с принятыми стандартами.

Эта модель описывает правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи. Основными элементами модели являются уровни, прикладные процессы и физические средства соединения.

Семиуровневая эталонная модель “Взаимосвязь открытых систем” была разработана с целью упрощения взаимодействия устройств в сетях.

Семиуровневая эталонная модель представляет собой рекомендации (разработчикам сетей и протоколов) для построения стандартов совместимых сетевых программных продуктов, и служит базой для производителей при разработке совместимого сетевого оборудования. Рекомендации стандарта должны быть реализованы как в аппаратуре, так и в программных средствах вычислительных сетей.

Семиуровневая эталонная модель OSI определяет семь уровней взаимодействия систем в сетях с коммуникацией пакетов, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень. Каждый уровень функционирует независимо от выше - и нижележащих уровней. Каждый уровень может общаться с непосредственным соседним уровнем, однако он полностью изолирован от прямого обращения к следующим уровням (рис.7).

Модель OSI делит сеть на семь функциональных уровней, поэтому ее иногда называют **семиуровневым стеком**.

Если протоколы работают в рамках семиуровневого стека, то на каждом уровне действуют одни и те же правила, создавая межпротокольную связь.

Каждый уровень имеет свой собственный протокол взаимодействия между устройствами (рис. 6). Для установки соединения в рамках стандартизированного взаимодействия каждый уровень обращается к другому уровню для управления определенным фрагментом сетевого соединения. Между уровнями всегда имеется фиксированный интерфейс, позволяя установку соединения с помощью различных протоколов.

Рисунок 7 – Модель OSI

1 уровень - физический.

Физический уровень предназначен для сопряжения с физическими средствами соединения. Физические средства соединения – это совокупность физической среды, аппаратных и программных средств, обеспечивающая передачу сигналов между системами. Физическая среда – это материальная субстанция, через которую осуществляется передача сигналов. Физическая среда является основой, на которой строятся физические средства соединения. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц.

Физический уровень выполняет следующие функции:

– Установление и разъединение физических соединений;
– Передача сигналов в последовательном коде и прием;
– Прослушивание, в нужных случаях, каналов;
– Идентификация каналов;
– Оповещение о появлении неисправностей и отказов.

Оповещение о появлении неисправностей и отказов связано с тем, что на физическом уровне происходит обнаружение определенного класса событий, мешающих нормальной работе сети (столкновение кадров, посланных сразу несколькими системами, обрыв канала, отключение питания, потеря механического контакта и т.п.). Виды сервиса, предоставляемого канальному уровню, определяются протоколами физического уровня. Прослушивание канала необходимо в тех случаях, когда к одному каналу подключается группа систем, но одновременно передавать сигналы разрешается только одной из них.

Можно считать, что уровень отвечает за аппаратное обеспечение.

Физический уровень может обеспечивать как асинхронную (последовательную) так и синхронную (параллельную) передачу, которая применяется для некоторых мэйнфреймов и мини – компьютеров.

2 уровень - канальный.

Единицей информации канального уровня являются кадры (frame). Кадры – это логически организованная структура, в которую можно помещать данные. Задача канального уровня – брать пакеты, поступающие с сетевого уровня и готовить их к передаче, укладывая в кадр соответствующего размера, а также проверять доступность среды передачи. Этот уровень обязан определить, где начинается и где заканчивается блок, а также обнаруживать и корректировать ошибки передачи.

Канальный уровень обеспечивает выполнение следующих функций:

– Организация (установление, управление, расторжение) канальных соединений и идентификация их портов;
– Организация и передача кадров;
– Обнаружение и исправление ошибок;
– Управление потоками данных;
– Обеспечение прозрачности логических каналов (передачи по ним данных, закодированных любым способом).

Наиболее часто используемые протоколы на канальном уровне включают:

– HDLC – протокол управления каналом передачи данных высокого уровня, для последовательных соединений;
– IEEE 802.2 LLC – протокол управления логическим каналом связи;
– Ethernet – сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей и обнаруживанием конфликтов;
– Token Ring – сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера;
– FDDI – сетевая технология по стандарту IEEE 802.6, использующая оптоволоконный носитель;
– X.25 – международный стандарт для глобальных коммуникаций с коммутацией пакетов;
– Frame relay – сеть, организованная из технологий X.25 и ISDN.

3 уровень - сетевой.

Сетевой уровень обеспечивает прокладку каналов, соединяющих абонентские и административные системы через коммуникационную сеть, выбор маршрута наиболее быстрого и надежного пути. Сетевой уровень устанавливает связь в вычислительной сети между двумя системами и обеспечивает прокладку виртуальных каналов между ними.

Виртуальный или логический канал – это такое функционирование компонентов сети, которое создает взаимодействующим компонентам иллюзию прокладки между ними нужного тракта. Кроме этого, сетевой уровень сообщает транспортному уровню о появляющихся ошибках. Сообщения сетевого уровня принято называть **пакетами**. В них

помещаются фрагменты данных. Сетевой уровень отвечает за их адресацию и доставку. Прокладка наилучшего пути для передачи данных называется **маршрутизацией**, и ее решение является главной задачей сетевого уровня.

Внутри сети доставка данных регулируется канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень.

При организации доставки пакетов на сетевом уровне используется понятие **номер сети.** В этом случае **адрес** получателя состоит из **номера сети** и **номера компьютера** в этой сети.

Сети соединяются между собой специальными устройствами, называемыми **маршрутизаторами.** Маршрутизатор – это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Таким образом, маршрут представляет собой последовательность маршрутизаторов, по которым проходит пакет. Сетевой уровень выполняет функции:

1. Создание сетевых соединений и идентификация их портов;
2. Обнаружение и исправление ошибок, возникающих при передаче через коммуникационную сеть;
3. Управление потоками пакетов;
4. Организация (упорядочение) последовательности пакетов;
5. Маршрутизация и коммутация;
6. Сегментирование и обьединение пакетов.

Наиболее часто на сетевом уровне используются протоколы:

– IP– протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию;

– IPX– протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пекетов в сетях Novell;

– X.25 – международный стандарт для глобальных коммуникаций с коммутацией пакетов;

4 уровень - транспортный.

Транспортный уровень предназначен для передачи пакетов через коммуникационную сеть. На транспортном уровне пакеты разбиваются на блоки. Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням модели (прикладному и сеансовому) передачу данных с той степенью надежности, которая им требуется.

Транспортный уровень определяет адресацию физических устройств в сети. Этот уровень гарантирует доставку блоков информации адресатам и управляет этой доставкой. Его **главной задачей** является обеспечение эффективных, удобных и надежных форм передачи информации между системами. Когда в процессе обработки находится более одного пакета, транспортный уровень контролирует очередность прохождения пакетов. Если проходит дубликат принятого ранее сообщения, то данный уровень опознает это и игнорирует сообщение.

В функции транспортного уровня входят:

1. Управление передачей по сети и обеспечение целостности блоков данных.
2. Обнаружение ошибок, частичная их ликвидация и сообщение о неисправных ошибках.
3. Восстановление передачи после отказов и неисправностей.
4. Укрупнение или разделение блоков данных.
5. Предоставление приоритетов при передаче блоков (нормальная или срочная).
6. Подтверждение передачи.
7. Ликвидация блоков при тупиковых ситуациях в сети.

Наиболее распространенные протоколы транспортного уровня:

– TCP – протокол управления передачей стека TCP/IP;

– UDP– пользовательский протокол дейтаграмм стека TCP/IP;

5 уровень - сеансовый.

Сеансовый уровень – это уровень, определяющий процедуру проведения сеансов между пользователями или прикладными процессами. Сеансовый уровень управляет передачей информации между прикладными процессами, координирует прием, передачу и выдачу одного сеанса связи. Кроме того, сеансовый уровень содержит дополнительно функции управления паролями, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях. Функции этого уровня состоят **в координации** связи между двумя прикладными программами, работающими на разных рабочих станциях. В число этих функций входит создание сеанса, управление передачей и приемом пакетов сообщений во время сеанса и завершение сеанса.

На сеансовом уровне определяется, какой будет передача между двумя прикладными процессами:

–**полудуплексной** (процессы будут передавать и принимать данные по очереди)**;**

– дуплексной (процессы будут передавать данные, и принимать их одновременно)**.**

Сеансовый уровень обеспечивает выполнение следующих функций:

– Установление и завершение на сеансовом уровне соединения между взаимодействующими системами;

– Выполнение нормального и срочного обмена данными между прикладными процессами;

– Управление взаимодействием прикладных процессов;

– Синхронизация сеансовых соединений;

– Извещение прикладных процессов об исключительных ситуациях;

– Установление в прикладном процессе меток, позволяющих после отказа либо ошибки восстановить его выполнение от ближайшей метки;

– Прерывание в нужных случаях прикладного процесса и его корректное возобновление;

– Прекращение сеанса без потери данных;

– Передача особых сообщений о ходе проведения сеанса.

6 уровень - уровень представлений.

Уровень представления данных или представительский уровень представляет данные, передаваемые между прикладными процессами, в нужной форме. Этот уровень обеспечивает то, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе.

Представительный уровень выполняет следующие функции:

1. Генерация запросов на установление сеансов взаимодействия прикладных процессов;
2. Согласование представления данных между прикладными процессами;
3. Реализация форм представления данных;
4. Представление графического материала (чертежей, схем, рисунков);
5. Засекречивание данных;
6. Передача запросов на прекращение сеансов;
7. Протоколы уровня представления данных обычно являются составной частью протоколов трех верхних уровней модели.

7 уровень - уровень приложений (или прикладной). В верхней части стека находятся протоколы, используемые для выполнения задач: SMTP для работы с электронной почтой, HTTP для веб-браузеров и серверов, Telnet для сеансов связи с удаленными терминалами и множество других.

Прикладной уровень - это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые WEB-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Специальные элементы прикладного сервиса обеспечивают сервис для конкретных прикладных программ, таких как программы пересылки файлов и эмуляции терминалов. Одна из основных задач этого

уровня – определить, как следует обрабатывать запрос прикладной программы, другими словами, какой вид должен принять данный запрос.

Прикладной уровень выполняет следующие функции:

1. Выполнение различных видов работ:

– передача файлов;

–управление заданиями;

– управление системой и т.д.

2. Идентификация пользователей по их паролям, адресам, электронным подписям.

3. Определение функционирующих абонентов и возможности доступа к новым прикладным процессам.

4. Определение достаточности имеющихся ресурсов.

5. Организация запросов на соединение с другими прикладными процессами.

6. Передача заявок представительскому уровню на необходимые методы описания информации.

7. Выбор процедур планируемого диалога процессов.

8. Управление данными, которыми обмениваются прикладные процессы и синхронизация взаимодействия прикладных процессов.

9. Определение качества обслуживания (время доставки блоков данных, допустимой частоты ошибок).

10. Соглашение об исправлении ошибок и определении достоверности данных.

11. Согласование ограничений, накладываемых на синтаксис (наборы символов, структура данных).

Примечание. Обратите внимание на правильное значение названия "уровень приложений"! Это сетевые приложения включают в себя электронную почту, веб-браузеры и протокол пересылки файлов (FTP).

Семиуровневая эталонная модель OSI описывает только системные средства взаимодействия, реализуемые операционной системой, системными утилитами, системными аппаратными средствами.

В соответствии с семиуровневой эталонной моделью сетевая система представляется прикладными процессами и процессами взаимодействия абонентов. Последние, разбиваются на семь функциональных уровней: прикладной, представительный (уровень представления данных), сеансовый, транспортный, сетевой, канальный и физический.

При запуске на компьютере любого приложения, для функционирования которого требуется диалог с сетью, это приложение вызывает соответствующий протокол прикладного уровня сетевого программного обеспечения. Прикладной уровень формирует сообщение стандартного формата. Обычно сообщение состоит из заголовка и поля данных.

Заголовок содержит служебную информацию, которую необходимо передать через сеть прикладному уровню компьютера-адресата, чтобы сообщить ему, какую работу надо выполнить. Поле данных содержит данные, необходимые для выполнения этой работы.

После формирования сообщения прикладной уровень направляет его вниз к представительному уровню. Представительный уровень, на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию – заголовок представительного уровня, в котором содержатся указания для представительного уровня машины-адресата.

Полученное сообщение отправляется вниз сеансовому уровню, который добавляет свой заголовок и т.д. до физического уровня, который передает сформированное сообщение по линиям связи. К этому моменту сообщение имеет заголовки всех уровней.

Когда сообщение поступает в компьютер - адресат, оно принимается физическим уровнем и последовательно передается вверх с уровня на уровень. Причем каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие данному уровню функции, а затем удаляет этот заголовок и передает сообщение вышележащему уровню.

Первые три уровня в этой модели (7,6,5) управляют используемым сетевым приложением (уровень приложений), форматом представления данных (уровень представлений) и характеристиками соединения (сеансовый уровень). Например, порт 25 идентифицирует SMTP-приложение электронной почты.

Примечание: порты – это логические зоны компьютера, где ожидается получение информации определенного типа.

При переходе на следующий уровень - *транспортный* - размер сообщения немного увеличивается. Здесь главная задача состоит в предоставлении принимающему компьютеру сведений о поступающем сообщении, а также в том, чтобы он не был перегружен пакетами. Кроме того, этот уровень дает гарантию того, что все передаваемые пакеты дойдут до получателя.

Следующий уровень, добавляемый к сообщению, - сетевой уровень. Именно на этом этапе сообщение превращается в пакет или дейтаграмму. В заголовок пакета включается логический сетевой адрес, по которому передается сообщение. В числе других сетевые протоколы включают в себя и протокол IP.

За сетевым уровнем следует канальный уровень. Здесь считываются данные, представленные в двоичном виде, и добавляются к формату, который называется кадром. Формат кадра задается протоколом сетевого адаптера (например, Ethernet или ATM). В заголовке каждого кадра содержится MAC-адрес (Media Access Control) - адрес управления доступом к среде для сетевого устройства. У каждого сетевого адаптера есть свой уникальный MAC-идентификатор.

На *физическом* уровне сообщение преобразуется в последовательность импульсов, передающих данные в двоичном виде.

Это последний уровень стека, и он не зависит от того, в каком виде передается сигнал, - в виде электрических импульсов обычной сети или световых импульсов оптоволоконной линии. Импульсы обрабатываются платами сетевого интерфейса, программное обеспечение сетевой среды в этом процессе не участвует.

Контрольные вопросы:

1.Семиуровневая эталонная модель OSI. Модель OSI-ISO. Перечень 7 функциональных уровней стека модели OSI

2.Функции 7,6 и 5 уровней

3.Функции транспортного уровня

4.Функции сетевого уровня

5.Функции канального и физического уровней

Практическое занятие 9
Объединение ЛВС. Корпоративные сети.

Цель: дать студенту основные сведения об устройствах объединения сетей, об устройствах территориально распределенных сетей; протоколах канального уровня, этапах построения корпоративных сетей; функции оборудования объединения сетей (коммутатор, роутер, мост и др.

Теоретическая часть:

Устройства объединения сетей. Протоколы канального уровня: Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface). Корпоративные сети, Этапы построения корпоративных сетей.

Устройства объединения сетей обеспечивают связь между сегментами локальных сетей, отдельными ЛВС и подсетями любого уровня. Эти устройства в самом общем виде могут быть отнесены к определенным уровням эталонной модели взаимодействия

открытых систем. Существуют следующие классы устройств для объединения сегментов ЛВС и сетей.

Сетевые коммутаторы

Не так давно для построения локальных сетей применялись сетевые ***концентраторы*** (или, в просторечии, ***хабы***). Когда сетевая карта отсылает пакет данных с компьютера в сеть, хаб просто усиливает сигнал и передает его всем участникам сети. Принимает и обрабатывает пакет только та сетевая карта, которой он адресован, остальные его игнорируют. По сути, концентратор – это усилитель сигнала.

В настоящее время в локальных сетях применяются **коммутаторы** (или, как их называют, ***свитчи***). Это более "интеллектуальные" устройства, где есть свой процессор, внутренняя шина и буферная память. Если концентратор просто передает пакеты от одного порта ко всем остальным, то коммутатор анализирует адреса сетевых карт, подключенных к его портам, и переправляет пакет только в нужный порт. В результате бесполезный трафик в сети резко снижается.

Коммутатор может работать на скорости 10, 100 или 1000 Мбит/с. Это, а также установленные на компьютерах сетевые карты, определяет скорость сегмента сети. Другая характеристика коммутатора – количество портов. От этого зависит количество сетевых устройств, которые можно подключить к коммутатору. Помимо компьютеров, ими являются принт-серверы, модемы, сетевые дисковые накопители и другие устройства с LAN-интерфейсом.

Коммутаторы бывают двух видов – управляемые и неуправляемые. Управляемые, обладают дополнительной функциональностью. Так, появляется возможность управления коммутатором с помощью веб-интерфейса, объединения нескольких коммутаторов в один виртуальный со своими правилами коммутации пакетов и т.д. Стоимость управляемых коммутаторов гораздо выше стоимости неуправляемых, поэтому в малых и средних сетях используются неуправляемые коммутаторы.

В локальной сети можно использовать различное дополнительное оборудование, например, чтобы объединить две сети или обеспечить защиту сети от внешних атак. Кратко рассмотрим сетевое оборудование, которое применяется при построении компьютерных сетей.

Принт-сервер, или **сервер печати** – это устройство, которое позволяет подключить принтер, не имеющий собственного сетевого порта к сети. Проще говоря: принт-сервер – это коробка, к которой с одной стороны подключается принтер, а с другой стороны — сетевой провод. При этом принтер становится доступным в любое время, поскольку не привязан к какому-либо компьютеру сети. Существуют принт-серверы с разными портами: USB и LPT; так же встречаются и комбинированные варианты.

Повторитель предназначен для увеличения расстояния сетевого соединения путем усиления электрического сигнала. Если вы будете использовать в локальной сети кабель витая пара длиной более 100 метров, повторители должны устанавливаться в разрыв кабеля через каждые 100 метров. Питание повторителей обычно осуществляется по тому же кабелю. С помощью повторителей можно соединить сетевым кабелем несколько отдельно стоящих зданий.

Маршрутизатор (или **роутер**) – сетевое устройство, которое на основании информации о структуре сети по определенному алгоритму выбирает маршрут для пересылки пакетов между различными сегментами сети.

Маршрутизаторы применяют для объединения сетей разных типов, зачастую несовместимых по архитектуре и протоколам (например, для подсоединения Ethernet к сети WAN). Также маршрутизатор используется для обеспечения доступа из локальной сети в глобальную сеть Интернет, осуществляя при этом функции межсетевого экрана.

Мост – устройство, объединяющее две идентичные сети простой конфигурации, использующие одинаковые методы передачи данных в пределах ограниченного пространства. Мост может соединять сети разных топологий, но работающие под управлением однотипных сетевых операционных систем.

Шлюз – устройство, позволяющее организовать обмен данными между различными сетями, использующими разные протоколы взаимодействия.

Шлюз выполняет преобразование между двумя протоколами для всех 7 уровней взаимодействия и позволяет подключить локальную сеть к глобальной сети

Протоколы канального уровня: Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface)

Если обмены у узлов появляются асинхронно, то возникает проблема разделения общей среды между многими узлами, другими словами, проблема обеспечения доступа к сети.

Доступом к сети называют взаимодействие узла сети со средой передачи данных для обмена информацией с другими узлами.

Управление доступом к среде - это установление последовательности, в которой узлы получают полномочия по доступу к среде передачи данных.

Методы доступа могут быть случайными или детерминированными.

- Основным используемым методом случайного доступа является метод множественного доступа с контролем несущей и обнаружением конфликтов (МДКН/ОК) или (**CSMA/CD).**
- Узел, желающий начать передачу, обнаружив в некоторый момент времени $\mathbf{t_1}$ отсутствие колебаний, захватывает свободную линию, т.е. получает полномочия по использованию линии. Любая другая станция, желающая начать передачу в момент времени $\mathbf{t_2 > t_1}$ при обнаружении электрических колебаний в линии, откладывает передачу до момента $\mathbf{t + t_d}$, где t_d - задержка.

Среди детерминированных методов доступа к сети передачи данных преобладают **маркерные методы доступа**. Маркерные методы основаны на передаче полномочий на передачу одному из узлов сети с помощью специального информационного объекта, называемого маркером.

Жизнедеятельность человека связана с разнообразными ресурсами: природными, материальными, энергетическими, финансовыми. В информационном обществе все более значимыми становятся информационные ресурсы. Они возникли как результат интеллектуальной деятельности человека, обладающего определенными знаниями и опытом. Эти знания материализуются в виде произведений искусства, литературы, научных разработок, баз данных, алгоритмов, компьютерных программ.

С распространением персональных компьютеров огромную роль в предоставлении человеку доступа к информационным ресурсам стали играть компьютерные сети (Computer NetWork, от англ. net — сеть и work — работа).

Корпоративные сети называют также сетями масштаба предприятия, что соответствует дословному переводу термина «enterprise-wide networks», используемого в англоязычной литературе для обозначения этого типа сетей. Сети масштаба предприятия (корпоративные сети) объединяют большое количество компьютеров на всех территориях отдельного предприятия. Они могут быть сложно связаны и покрывать город, регион или даже континент. Число пользователей и компьютеров может измеряться тысячами, а число серверов - сотнями, расстояния между сетями отдельных территорий могут оказаться такими, что становится необходимым использование глобальных связей. Для соединения удаленных локальных сетей и отдельных компьютеров в корпоративной сети применяются разнообразные телекоммуникационные средства, в том числе телефонные каналы, радиоканалы, спутниковая связь. Корпоративную сеть можно представить в виде «островков локальных сетей», плавающих в телекоммуникационной среде.

В корпоративной сети обязательно будут использоваться различные типы компьютеров - от мэйнфреймов до персоналок, несколько типов операционных систем и множество различных приложений. Неоднородные части корпоративной сети должны работать как единое целое, предоставляя пользователям по возможности прозрачный доступ ко всем необходимым ресурсам.

При переходе от более простого типа сетей к более сложному, от сетей отдела к корпоративной сети - сеть должна быть все более надежной и отказоустойчивой, при этом

требования к ее производительности также существенно возрастают. По мере увеличения масштабов сети увеличиваются и ее функциональные возможности. По сети циркулирует все возрастающее количество данных, и сеть должна обеспечивать их безопасность и защищенность наряду с доступностью. Соединения, обеспечивающие взаимодействие, должны быть более прозрачными. При каждом переходе на следующий уровень сложности компьютерное оборудование сети становится все более разнообразным, а географические расстояния увеличиваются, делая достижение целей более сложным; более проблемным и дорогостоящим становится управление такими соединениями.

Территориально-распределенные сети (КСПД), построенные на основе технологии VPN, являются фундаментом для внедрения всех последующих дополнительных сервисов, таких как передача голоса по IP, видеоконференц-связь, бизнес-приложения и сервисы, а также для организации оперативной и конфиденциальной связи со всеми филиалами компании и значительного уменьшения объема междугороднего и международного трафика за счет передачи телефонных звонков по каналам КСПД.

Контрольные вопросы:

1. Устройства объединения сетей.
2. Функции коммутатора, принт-сервера, повторителя, маршрутизатора, роутера, моста и шлюза.
3. Функции протоколов канального уровня
4. Отличия корпоративной сети от локальной и глобальной сетей.

Практическое занятие 10
Территориально распределенные вычислительные сети. Принципы построения.

Цель: дать студенту основные сведения об устройствах объединения сетей, об устройствах территориально распределенных сетей; протоколах канального уровня, этапах построения корпоративных сетей; функции оборудования территориально распределенных сетей, функции протоколов канального уровня; использовать средства объединения сетей, использовать средства территориально распределенных сетей.

При переходе от более простого типа сетей к более сложному - от сетей отдела к корпоративной сети - сеть должна быть все более надежной и отказоустойчивой, при этом, требования к ее производительности также существенно возрастают. Неоднородные части корпоративной сети должны работать как единое целое, предоставляя пользователям по возможности прозрачный доступ ко всем необходимым ресурсам. Это можно обеспечить только с помощью подбора оборудования сетей.

Территориально-распределенные сети (КСПД) – из названия очевидно, что данный тип сетей связи – это сетевая структура, объединяющая с помощью различных каналов связи офисы и здания одной компании, которые расположены на значительном отдалении друг от друга.

Территориально-распределенные сети (КСПД), как правило, объединяют офисы, подразделения и другие структуры компании, находящиеся на удалении друг от друга. При этом часто узлы корпоративной сети оказываются расположенными в различных городах, а иногда и странах.

Принципы, по которым строится такая сеть, отличаются от тех, что используются при создании локальных сетей (рис.8).

Основное отличие состоит в том, что территориально-распределенные сети используют арендованные линии связи, арендная плата за использование которых

составляет значительную часть в себестоимости всей сети и возрастает с увеличением качества и скорости передачи данных.

Поэтому организация каналов связи является первой задачей, которую необходимо решать при создании территориально-распределенных корпоративных сетей. Если в пределах одного города возможна аренда выделенных линий, в том числе высокоскоростных, то при переходе к географически удаленным узлам стоимость аренды каналов становится значительной, а их качество и надежность при этом могут быть невысокими.

Возможным решением задачи организации каналов связи между удаленными узлами корпоративной сети компании является использование уже существующих глобальных частных сетей. В этом случае необходимо обеспечить каналы от офисов компании до ближайших узлов глобальной частной сети. Частные сети могут содержать каналы связи разных типов: кабельные оптические и электрические, в том числе телефонные, беспроводные радио- и спутниковые каналы, имеющие различные пропускные способности.

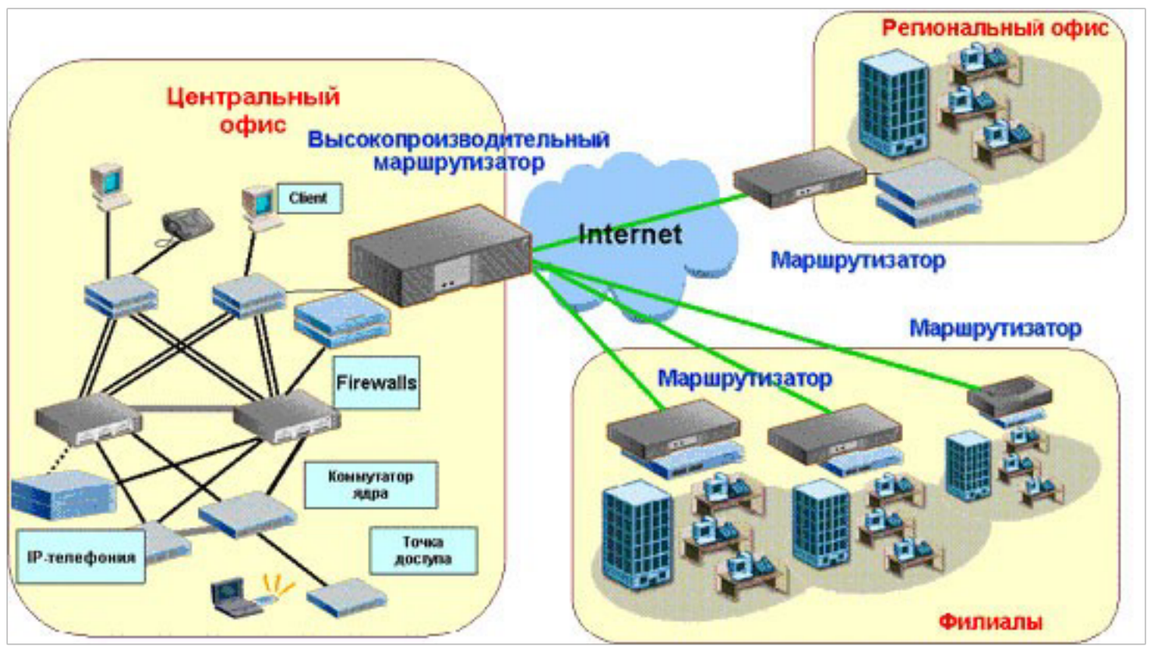


Рисунок 8- Принцип построения сети

При подключении офисов компании через глобальные частные сети удаленные пользователи не ощущают себя изолированными от информационных систем, к которым они осуществляют доступ, удаленные местоположения компании могут осуществлять обмен информацией незамедлительно, и вся передаваемая информация остается в секрете. Однако организация каналов связи через глобальные частные сети также может быть дорогостоящей.

Обеспечить многие преимущества частных сетей за меньшую стоимость позволяет **технология виртуальных частных сетей** (VPN, Virtual Private Network).

VPN – это логическая частная сеть, организуемая поверх публичной сети, как правило, сети Интернет. Следуя тем же функциональным принципам, что и выделенные линии, VPN позволяет установить защищённое цифровое соединение между двумя удаленными местоположениями (или локальными сетями). Несмотря на то, что по публичным сетям коммуникации осуществляются с использованием небезопасных протоколов, за счёт шифрования создаются закрытые каналы обмена информацией, обеспечивающие безопасность передаваемых данных (рис.9).

Виртуальные частные сети позволяют объединить географически распределенные офисы организации в единую сеть и таким образом обеспечить единое адресное пространство ЛВС, единую нумерацию корпоративной телефонной связи, общую базу данных и т.д. Иными словами, организуется единая сетевая инфраструктура и информационное пространство компании, доступ к которому одинаково возможен из любой точки корпоративной сети.

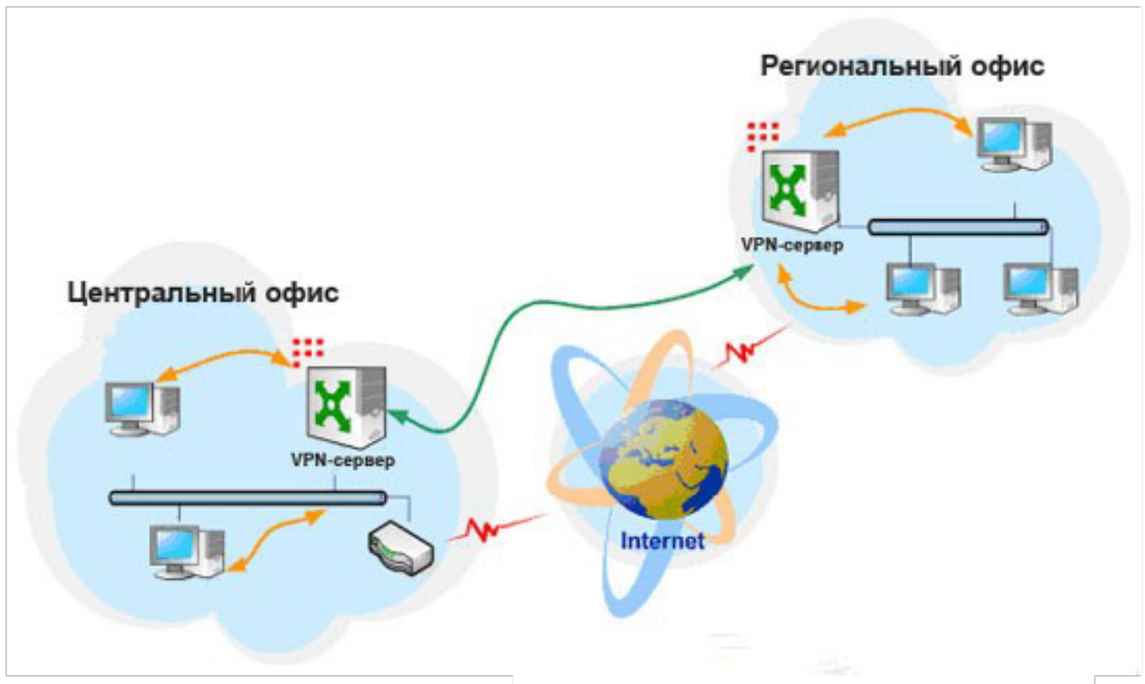


Рисунок 9 – Пример виртуальной частной сети

Контрольные вопросы

5. Принципы построения территориально-распределенных сетей
6. Технология виртуальных частных сетей VPN.
7. Основное отличие территориально-распределенных сетей

Практическое занятие 11
Разработка топологии иерархической сети.

Цель: дать студенту сведения о топологии иерархической сети, функции топологии иерархической сети

Теоретическая часть:

Концепция иерархических сетей очень напоминает концепцию эталонной модели OSI, в соответствии с которой процесс взаимодействия между компьютерами разбивается на несколько функциональных уровней, выполняющих определенный круг задач. Уровни иерархической модели должны как можно более точно соответствовать поставленным перед ними целям.

Иерархическая топология также называется вертикальной, или древовидной, сетью. Слово «дерево» связано с тем фактом, что иерархическая сеть часто напоминается дерево, ветви которого растут из вершины вниз до самого нижнего уровня.

Иерархические сети строятся на базе техники кабельного телевидения. Основные преимущества таких сетей - относительно большая протяженность (до 50 км) и возможность параллельной передачи речи, данных и изображений. Возможности по наращиванию иерархической сети весьма ограничены из-за высокой стоимости ее установки и сложности аналоговых компонентов, которые требуют, кроме того, регулярной настройки. Перед развертыванием сети необходима предварительная тщательная проработка трасс кабелей, мест установки ретранслятора, усилителей, ответвителей, учитывающая перспективы подключения новых оконечных систем.

Надежность иерархической сети обеспечивается, как правило, резервированием ее связных устройств, время наработки на отказ которых может составлять до 400 тыс. часов.

В большинстве случаев иерархическая модель сети подразумевает определение трех уровней. Как показано на рисунке 10, каждый уровень иерархической сети выполняет собственные функциональные задачи.

Ядро (core) сети отвечает за высокоскоростную передачу сетевого трафика; первичное предназначение устройства, входящего в ядро сети, заключается в коммутации пакетов.

На *уровне распределения (access layer)* происходит суммирование маршрутов и агрегация трафика.

Уровень доступа (access 1ayer) отвечает за формирование сетевого трафика, выполняет контроль точек входа в сеть и предоставляет другие службы пограничных устройств.

Посмотрим на взаимоотношение этих уровней с фундаментальных принципов проектирования сетей.

1. Размеры участка сети, на которые влияет изменение топологии, должны быть строго ограничены; при этом желательно, чтобы данный участок сети был как можно меньшим.
2. Маршрутизаторы (а также другие сетевые устройства) должны обрабатывать минимально возможный объем информации.

Каждый из этих принципов может быть реализован с помощью суммирования, которое осуществляется на уровне распределения иерархической модели сети. Таким образом, отсюда следует, что область сходимости протокола маршрутизации должна быть ограничена уровнем распределения.

Так, повреждение канала передачи информации уровня доступа, не должно стать причиной изменения таблицы маршрутизации ядра и наоборот – повреждение линии связи ядра не должно оказать сколько-нибудь значительного влияния на таблицы маршрутизации устройств уровня доступа.

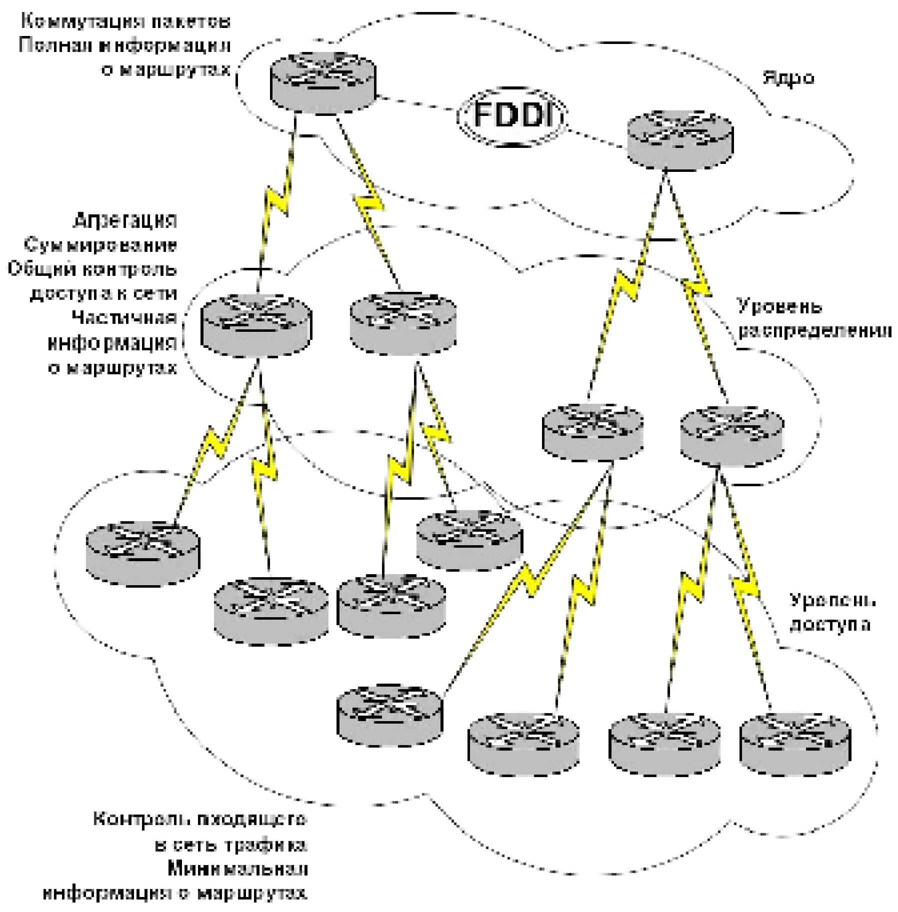


Рисунок 10 – Структура иерархической сети

В иерархических сетях агрегация трафика и его направление в высокоскоростные каналы передачи информации происходит по мере продвижения трафика от уровня доступа к ядру сети. Аналогично разделение трафика и его направление по менее скоростным каналам передачи данных происходит по мере продвижения трафика от ядра сети к устройствам уровня доступа, как показано на рисунке 11.

Ядро сети

Перед ядром сети поставлена одна четко сформулированная задача – коммутация пакетов (switching packets). Устройства ядра должны функционировать в режиме пиковой производительности. Именно в ядре сети сосредоточена вся ее вычислительная мощность.

Основные стратегии, позволяющие добиться максимальной производительности ядра сети:

1. В ядре не должны реализовываться сетевые правила.
2. Каждое устройство ядра должно обладать возможностью доступа к каждому пункту назначения сети.

Полная достижимость каждого пункта назначения

Устройства ядра должны обладать достаточной информацией о маршрутах для проведения интеллектуальной коммутации пакета, предназначенного для любого конечного устройства сети; маршрутизаторы ядра не должны использовать стандартные маршруты для достижения внутренних пунктов назначения. Следует отметить, сказанное выше отнюдь не означает, что маршрутизатор ядра должен обладать сведениями о маршруте к каждой отдельной подсети. Для уменьшения размеров таблицы

маршрутизации ядра могут и должны использоваться суммарные маршруты. Стандартные же маршруты следует использовать для достижения внешних пунктов назначении, таких, например, как узлы Internet.

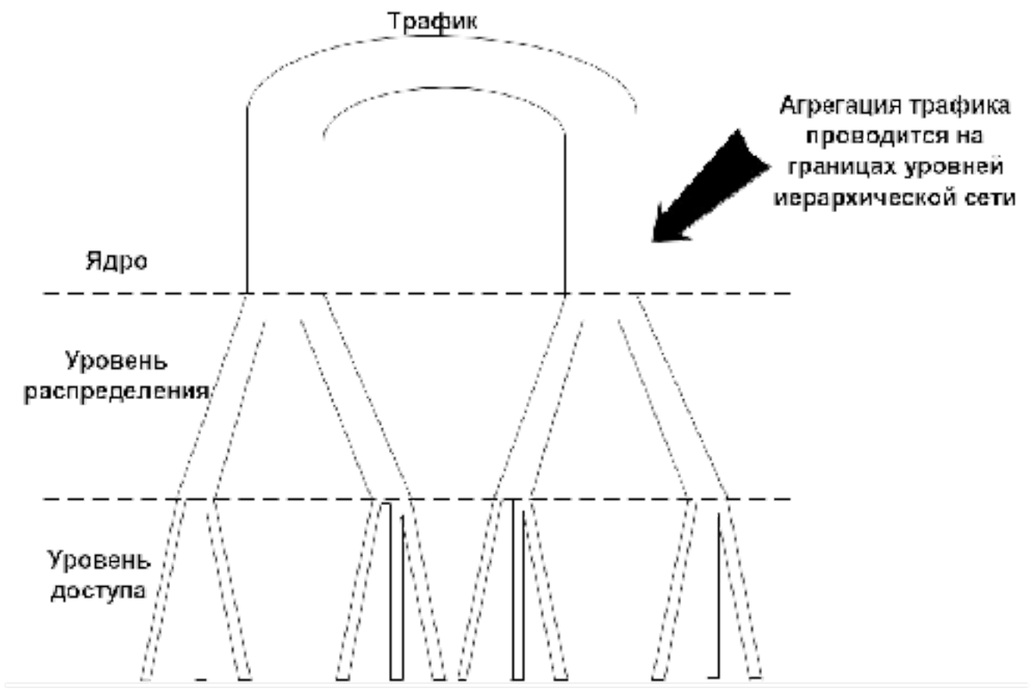


Рисунок 11 – Агрегации трафика и суммирование маршрутов на границах уровней

Существует три основные причины для отказа от стратегии стандартных маршрутов:

1. Облегчение задачи обеспечения избыточности ядра.
2. Снижение вероятности частично оптимизированной маршрутизации.
3. Предотвращение возникновения петель маршрутизации.

Поскольку объем трафика достигает максимума именно в ядре, здесь необходимо учитывать каждое принятие решения о коммутации пакетов. Учитывая специфику ядра, частично оптимизированная маршрутизация может явиться причиной дестабилизации сети.

Примером данной стратегии является структура точек доступа к сети (Network Access Points) в Internet. Устройствам, подключенным к точкам доступа к сети, не разрешается использовать стандартные маршруты для достижения, какого бы то ни было пункта назначения. Следовательно, каждое подключенное устройство *должно* поддерживать полную таблицу маршрутизации Internet. Необходимо отметить, что полная таблица маршрутизации не включает в себя информацию о маршруте к каждой возможной подсети. Вместо этого на уровне распределения сети (куда входят маршрутизаторы, поставляющие трафик в точку доступа к сети) активно используется агрегация, позволяющая эффективно уменьшить размер таблицы маршрутизации Internet в ядре.

Типы ядра

В большинстве малых сетей используется *вырожденный* тип ядра. Вырожденное ядро состоит из одного маршрутизатора, выполняющего роль ядра сети и соединенного со всеми остальными маршрутизаторами уровня распределения. В совсем мелких сетях маршрутизатор вырожденного ядра может быть подключен непосредственно к маршрутизаторам уровня доступа, минуя, таким образом, уровень распределения, который зачастую просто отсутствует в сетях малого размера.

Вырожденные ядра легко поддаются обслуживанию, так как дело приходится иметь всего лишь с одним маршрутизатором, однако достаточно негативно влияют на возможность масштабирования сети. Основной причиной плохой масштабируемости сетей с вырожденным ядром является необходимость прохождения каждого пакета сети через центральный маршрутизатор, что в конечном итоге может вызвать перегрузку даже самых больших и быстрых маршрутизаторов. К сожалению, необходимо также отметить очень тесную связь понятия вырожденного ядра с понятием одиночной точки отказа, которая весьма лаконично может быть описана следующим законом Мерфи: «Вышедший из строя маршрутизатор сети обязательно окажется маршрутизатором вырожденного ядра».

Поскольку вырожденное ядро с одним маршрутизатором не соответствует потребностям крупной сети, в большинстве корпоративных сетей используется группа маршрутизаторов, соединенных между собой высокоскоростной локальной сетью (Local Area Network – LAN), или объединение высокоскоростных каналов глобальных сетей (Wide Area Network – WAN), которые формируют ядро сети. Использование базовой сети вместо единственного маршрутизатора в качестве ядра позволяет предусмотреть избыточность еще на этапе проектирования и сохраняет возможность масштабирования сети путем добавления в ядро новых маршрутизаторов и каналов передачи информации.

Довольно часто удачно спроектированная базовая сеть поддается обслуживанию так же легко, как и ядро, состоящее из одного маршрутизатора (вырожденное ядро). К тому же базовая сеть более устойчива по отношению к различным неисправностям и гораздо лучше масштабируется, чем ядро, состоящее из одного маршрутизатора.

Уровень распределения

Перед уровнем распределения сети поставлено три четко сформулированные задачи:

1. Изоляция последствий изменения топологии.
2. Управление размером таблицы маршрутизации.
3. Агрегация сетевого трафика.

Для достижения этих целей используются две основные стратегии, реализуемые на уровне распределения:

1. Суммирование маршрутов.
2. Минимизация числа каналов, соединяющих уровень распределения с ядром сети.

Уровень распределения отвечает за агрегацию сетевого трафика. Агрегация достигается за счет объединения трафика, поступающего по большому числу низкоскоростных каналов передачи информации, связывающих уровень распределения с устройствами уровня доступа, в несколько широкополосных каналов, связывающих уровень распределения с ядром сети. Подобная стратегия порождает в сети эффективные точки суммирования и уменьшает количество маршрутов, которое должны принимать во внимание маршрутизаторы ядра при принятии решения о коммутации пакетов.

Уровень доступа

Перед уровнем доступа сети поставлено три основные задачи:

1. Формирование сетевого трафика.
2. Контроль доступа к сети.
3. Выполнение других функций пограничных устройств.

Устройства уровня доступа соединяют высокоскоростные каналы локальных сетей с каналами глобальной сети, несущими трафик на уровень распределения. Устройства уровня доступа представляют собой видимую часть сети; именно они ассоциируются у большинства заказчиков с понятием «сеть».

Формирование сетевого трафика

Следует обязательно убедиться в том, что трафик, сформированный на уровне доступа сети, не перегружает канал, соединяющий уровень доступа с уровнем распределения. Несмотря на то, что эта задача решается главным образом на этапе определения пропускной способности канала передачи информации, она имеет отношение к расположению пары «сервер-служба» и фильтрации пакетов. Трафик, не предназначенный для использования за пределами локальной сети, не должен передаваться устройством уровня доступа.

Никогда не используйте устройства уровня доступа в качестве промежуточной точки при передаче транзитного трафика между двумя маршрутизаторами уровня распределения, а именно такая ситуация свойственна сетям с высокой степенью избыточности.

Контроль доступа сети

Будучи местом фактического подключения заказчиков к сети, уровень доступа является отличной платформой для злоумышленников, которые пытаются незаконным

образом проникнуть в сеть. Для того чтобы блокировать подозрительный трафик, включая пакеты, источником которых является узел за пределами локальной сети, необходимо воспользоваться фильтрацией пакетов. Фильтрация пакетов позволяет предотвратить множество различных типов атак, исходящих из уязвимых сегментов сети, в основе которых лежит подмена адресов источников. Помимо этого уровень доступа предоставляет прекрасную возможность реализовать фильтрацию пакетов, защищающую подключенные к локальному сегменту устройства от атак извне (или даже изнутри) вашей сети.

Несмотря на то, что большая часть мер безопасности реализуется на участке соединения сети с внешним миром, в частности с Internet, фильтрация пакетов на уровне доступа, которая позволяет регулировать входящий трафик, может значительно повысить безопасность всей сети.

Таблица 1.1 – Цели и стратегии уровней иерархической модели сети

Уровень	Цели	Стратегии
Ядро сети	Скорость коммутации пакетов	Полная достижимость: запрет на использование стандартных маршрутов для достижения внутренних пунктов назначения и уменьшение частично оптимизированной маршрутизации. *Запрет на реализацию сетевых правил:* запрет контроля за доступом к сети, запрет на реализацию сетевых правил, а также уменьшение загрузки процессора и памяти
Уровень распределения	Локализация участка сети, на который влияет изменение топологии; управление размером таблицы маршрутизации; агрегация трафика	*Суммирование маршрутов:* локализация участка сети, на который влияет изменение топологии, сокрытие детальной информации о маршрутах от устройств ядра сети и устройств уровня доступа *Минимизация числа каналов, соединяющих уровень распределения с ядром:* уменьшение сложности принятия решения о коммутации пакета и создание предпосылок для проведения суммирования маршрутов и агрегации трафика
Уровень доступа	Формирование сетевого трафика; контроль доступа к сети	Предотвращение транзитного трафика. Фильтрация пакетов. В число других служб пограничных устройств входит маркировка пакетов для маршрутизации, осуществляемой в соответствии с критерием качества обслуживания (QoS), и уничтожение туннелей.

Одна из основных задач при построении ЛВС является выбор принципов маршрутизации пакетов с учетом особенности маршрутизации в сетях с интеграцией услуг и особенности реализации механизмов эстафетной передачи в беспроводных сетях с интеграцией услуг.

Контрольные вопросы

1. Почему топология сети имеет такое большое значение?
2. Являются ли топология сети и логическая структура сети взаимозаменяемыми понятиями?
3. Почему иерархические сети состоят из нескольких «уровней»?
4. Назовите уровень сети, на котором должны выполняться приведенные ниже функции/службы:

а) суммирование набора сетей назначения для снижения объема информации, обрабатываемой маршрутизаторами;

б) маркировка пакетов для проведения маршрутизации, осуществляемой в соответствии с критерием качества обслуживания;

в) снижение загрузки маршрутизаторов и каналов передачи информации в целях проведения максимально быстрой коммутации пакетов;

г) измерение объема трафика;

д) использование стандартного маршрута для достижения внутренних пунктов назначения;

е) контроль поступающего в сеть трафика с помощью фильтрации пакетов;

5.Какова первичная цель ядра сети? Какие стратегии используются для достижения этой цели?

6.Назовите первичные цели уровня доступа сети.

Практическое занятие 12
Маршрутизация в сетях.

Цель: дать студенту основные сведения об особенностях маршрутизации в сетях с интеграцией услуг, особенности реализации механизмов эстафетной передачи в беспроводных сетях с интеграцией услуг; основные сведения о принципах маршрутизации; алгоритмы маршрутизации, принципы маршрутизации пакетов.

Функциональная модель маршрутизатора

Маршрутизация решает две задачи:

1.выбор оптимального по некоторому критерию пути продвижения информации от источника к пункту назначения через объединенную сеть;

2.транспортировка информационных блоков (пакетов) по выбранному маршруту, или коммутация.

Определение оптимального маршрута

1.Критерий оптимальности маршрута может использовать различные показатели (длину, стоимость маршрута и т.д.).

2.Алгоритмы маршрутизации заполняют и поддерживают таблицы маршрутизации, в которых содержится информация необходимая для выбора маршрута.

3.Таблица маршрутизации, кроме различных показателей, необходимых для оптимизации маршрутов, содержит также результаты расчета оптимальных маршрутов в виде пар "Сеть назначения/Следующий узел".

Для определения оптимальных маршрутов к пунктам назначения, а также для поддержания и обновления своих маршрутных таблиц необходима полная информация о топологии сети. Для этого маршрутизаторы общаются друг с другом путем обмена специальными сообщениями:

а) сообщениями об обновлении маршрутизации, включающими всю маршрутную таблицу или ее часть, что позволяет каждому маршрутизатору построить полную картину топологии сети;

б) объявлениями о состоянии канала, содержащими информацию о состоянии каналов отправителя, которая также необходима маршрутизаторам для построения детальной топологии сети.

Алгоритмы маршрутизации

Как правило, хост-источник определяет необходимость отправки пакета в другой хост и поэтому отправляет пакет, адресованный в физический адрес своего маршрутизатора (уровень MAC), однако с сетевым адресом (адресом протокола) хоста пункта назначения.

Маршрутизатор отсылает пакет к следующему маршрутизатору путем замены физического адреса пункта назначения на физический адрес следующего маршрутизатора.

Следующая пересылка может быть в хост-пункт назначения или в очередной промежуточный маршрутизатор. По мере продвижения пакета через объединенную сеть, его физический адрес меняется, однако адрес протокола остается неизменным.

Хост (от англ. host —«хозяин, принимающий гостей») — любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый к локальной или глобальной сети.

Слово «хост» само по себе является практически жаргонным термином, и не несёт никакой информации об устройстве или его функционировании. Употребление слова «хост» имеет смысл только вместе с пояснением, хостом какого сервиса предполагается называемое устройство. Тем не менее, зачастую название сервиса опускают, предполагая, что оно очевидно из контекста.

Например, в реализации протокола USB управлением и координацией каждой группы клиентских устройств занимается отдельный USB Host Controller. В данном случае он выступает в качестве хоста протокола USB.

Чаще всего, однако, под «хостом» без дополнительных комментариев подразумевается хост протокола TCP/IP, то есть сетевой интерфейс устройства, подключённого к IP-сети. Как и всякий другой хост, этот имеет уникальное определение в среде сервисов TCP/IP (IP-адрес). С хостом протокола TCP/IPможет быть также связана необязательная текстовая характеристика — доменное имя.

В компьютерных играх и других сетевых приложениях, где подключение по сети создаётся динамически, под хостом обычно подразумевают того из участников соединения, который организует управление сеансом связи, в противовес остальным, которые подключаются к организованному им сеансу.

В соответствии со стандартами ISO, в больших сетях маршрутизация и коммутация организованы по иерархическому принципу. Для этого вводятся понятия:

– конечная система (End System - ES) - любой узел сети, который не занимается маршрутизацией, т.е. устройство сети, не обладающее способностью пересылать пакеты между подсетями;

– промежуточная система (Intermediate System - IS) - маршрутизатор, т.е. устройство сети, способное пересылать пакеты между подсетями;

– область (Area) - группа смежных сетей и подключенных к ним хостов, которые определяются как область администратором сети или другим аналогичным лицом;

– домен (Domain) - набор соединенных областей. Домены маршрутизации обеспечивают полную связность со всеми конечными системами, находящимися в их пределах.

Промежуточные системы далее подразделяются на следующие виды:

• внутридоменные IS, т.е. системы, которые могут сообщаться в пределах автономных систем (Autonomous System - AS) или доменов маршрутизации;

• междоменные IS, т.е. системы, которые могут сообщаться как в пределах домена маршрутизации, так и с другими доменами маршрутизации.

Промежуточные системы далее подразделяются на следующие виды:

• внутридоменные IS, т.е. системы, которые могут сообщаться в пределах автономных систем (Autonomous System - AS) или доменов маршрутизации;

• междоменные IS, т.е. системы, которые могут сообщаться как в пределах домена маршрутизации, так и с другими доменами маршрутизации.

IP-маршрутизация

Модуль IP и его таблица маршрутизации являются основным элементом межсетевого протокола IP. При статической маршрутизации содержание таблицы

определяется администратором сети. Протокол IP использует эту таблицу при принятии решений о маршрутизации IP-пакетов.

Правила (алгоритм) маршрутизации в модуле IP:

• Для отправляемых IP-пакетов, поступающих от модулей верхнего уровня, модуль IP определяет способ доставки - прямой или косвенный - и на основании результатов поиска в таблице маршрутизации выбирает сетевой интерфейс.

• Для принимаемых IP-пакетов, поступающих от сетевых драйверов, модуль IP решает, нужно ли ретранслировать IP-пакет по другой сети или необходимо передать его на верхний уровень. Принимаемый IP-пакет никогда не ретранслируется через тот же сетевой интерфейс, через который он был принят. Ретранслируемые пакеты обрабатываются далее также, как и отправляемые IP-пакеты.

• Решение о маршрутизации принимается до того, как IP-пакет передается сетевому драйверу, и до того, как происходит обращение к ARP-таблице.

Иерархическая маршрутизация

• Основное преимущество иерархической маршрутизации заключается в том, что она согласуется с организацией большинства компаний и, следовательно, очень хорошо поддерживает их схемы трафика.

• Большая часть сетевых коммуникаций осуществляется в пределах групп небольших подразделений компании (доменов).

• Внутридоменным маршрутизаторам достаточно иметь информацию только о других маршрутизаторах в пределах своего домена, поэтому их алгоритмы маршрутизации могут быть упрощенными и, соответственно, уменьшен трафик корректировки маршрутизации.

• Стандарт OSI предлагает протокол IS-IS внутридоменной маршрутизации промежуточных систем (Intermediate System to Intermediate System Intra-Domain Routing Exchange Protocol) и протокол ES-IS, вырабатывающий так называемые сообщения конфигурации (см. ниже).

Основные требования к алгоритмам маршрутизации:

• точность;
• простота;
• надёжность;
• стабильность;
• справедливость;
• оптимальность.

Существуют различные алгоритмы построения таблиц для одношаговой маршрутизации. Их можно разделить на три класса:

• алгоритмы простой маршрутизации;
• алгоритмы фиксированной маршрутизации;
• алгоритмы адаптивной маршрутизации.

Независимо от алгоритма, используемого для построения таблицы маршрутизации, результат их работы имеет единый формат. За счет этого в одной и той же сети различные узлы могут строить таблицы маршрутизации по своим алгоритмам, а затем обмениваться между собой недостающими данными, так как форматы этих таблиц фиксированы. Поэтому маршрутизатор, работающий по алгоритму адаптивной маршрутизации, может снабдить конечный узел, применяющий алгоритм фиксированной маршрутизации, сведениями о пути к сети, о которой конечный узел ничего не знает.

Простая маршрутизация

Это способ маршрутизации не изменяющийся при изменении топологии и состоянии сети передачи данных (СПД).

Простая маршрутизация обеспечивается различными алгоритмами, типичными из которых являются следующие:

• Случайная маршрутизация.
• Лавинная маршрутизация.
• Маршрутизация по предыдущему опыту.

В целом, простая маршрутизация не обеспечивает направленную передачу пакета и имеет низкую эффективности. Основным ее достоинством является обеспечение устойчивой работы сети при выходе из строя различных частей сети.

Фиксированная маршрутизация

Этот алгоритм применяется в сетях с простой топологией связей и основан на ручном составлении таблицы маршрутизации администратором сети.

Адаптивная маршрутизация

Это основной вид алгоритмов маршрутизации, применяющихся маршрутизаторами в современных сетях со сложной топологией. Адаптивная маршрутизация основана на том, что маршрутизаторы периодически обмениваются специальной топологической информацией об имеющихся в интерсети сетях, а также о связях между маршрутизаторами. Обычно учитывается не только топология связей, но и их пропускная способность и состояние.

Контрольные вопросы

4. Функциональная модель маршрутизатора.
5. Алгоритмы маршрутизации.
10. IP-маршрутизация
11. Иерархическая маршрутизация
12. Алгоритмы простой маршрутизации.
17. Иерархическая маршрутизация.

Практическое занятие 13
Сети с коммутацией каналов, пакетов, сообщений: ISDN, Frame Relay.

Цель: дать студенту основные сведения о каналах передачи данных, о сетях ISDN, о сети ретрансляции кадров Frame Relay; принципы работы каналов передачи данных, асинхронной передача данных, ATM – технологии.

Теоретическая часть:

Знание характеристик современных технологий позволяют решить основную задачу построения ЛВС - эффективная передача данных в сетях.

Канал передачи данных (ПД) - средства двустороннего обмена данными, включающие АКД и линию передачи данных.

В зависимости от способа представления информации электрическими сигналами различают *аналоговые* и *цифровые* каналы передачи данных.

В аналоговых каналах для согласования параметров среды и сигналов применяют *амплитудную, частотную, фазовую и квадратурно-амплитудную модуляции*.

В цифровых каналах для передачи данных используют *самосинхронизирующиеся коды*, а для передачи аналоговых сигналов - *кодово-импульсную модуляцию*.

В зависимости от направления передачи различают каналы *симплексные* (односторонняя передача), *дуплексные* (возможность одновременной передачи в обоих направлениях) и *полудуплексные* (возможность попеременной передачи в двух направлениях).

Если между двумя абонентами установлена постоянная связь, то канал называют выделенным, или постоянным. Такой канал может быть собственным или абонируемым.

Если соединение между абонентами устанавливают каждый раз при передаче данных, то такой канал называют коммутируемым. Для таких каналов существуют три этапа передачи данных:

1. Установка соединения;
2. Собственно передачи данных;

3. Разрыв соединения после окончания передачи данных.

К достоинствам выделенного канала относятся высокая скорость передачи данных, высокое качество сигналов, отсутствие блокировок, малое время, требуемое для установки соединения между абонентами сети. К недостаткам же такого канала относят высокую стоимость передачи информации и отсутствие гибкости.

Коммутируемый канал также имеет ряд достоинств, среди них: гибкость и невысокая стоимость передачи данных. А недостатки таких каналов в том, что возможны блокировки, качество передачи невысокое, а стоимость передачи информации в случае ее большого объема, напротив, высока.

Наиболее перспективными **сетями интегрального обслуживания** являются *сети с цифровыми каналами передачи данных,* например, **сети ISDN** (Рисунок 15).

Сети ISDN могут быть коммутируемыми и некоммутируемыми. Различают обычные ISDN со скоростями от 56 кбит/с до 1,54 Мбит/с и широкополосные ISDN (Broadband ISDN, или B-ISDN) со скоростями 155... 2048 Мбит/с. Более перспективны B-ISDN, в настоящее время технология B-ISDN активно осваивается.

Применяют два варианта обычных сетей ISDN - *базовый* и *специальный*. В базовом варианте имеются два канала по 64 кбит/с (эти каналы называют *B* каналами) и один служебный канал с 16 кбит/с (*D* канал). В специальном варианте - 23 канала *B* по 64 кбит/с и один или два служебных канала *D* по 16 кбит/с. Каналы *B* могут использоваться как для передачи закодированной голосовой информации (коммутация каналов), так и для передачи пакетов. Служебные каналы используются для сигнализации - передачи команд, в частности, для вызова соединения.

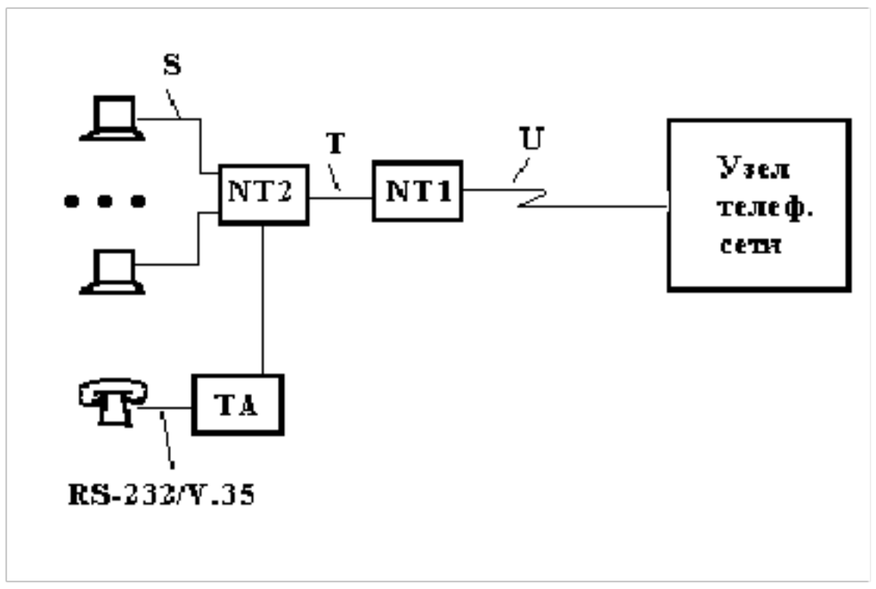


Рисунок 15 – Пример сети ISDN

Здесь S-соединение - 4-проводная витая пара. Если оконечное оборудование не имеет интерфейса ISDN, то оно подключается к S через специальный адаптер TA. Устройство NT2 объединяет S-линии в одну T-шину, которая имеет два провода от передатчика и два - к приемнику. Устройство NT1 реализует схему эхо-компенсации и служит для интерфейса T-шины с обычной телефонной двухпроводной абонентской линией U.

Сеть ретрансляции кадров Frame Relay.

Технология ретрансляции кадров Frame Relay применяется для передачи данных в крупных сетях (рисунок 16).

Технология, которая впоследствии, получила название Frame Relay (Коммутация кадров), первоначально была разработана вначале 1980-х для использования в сетях ISDN. Технология Frame Relay обеспечивает информационное взаимодействие на физическом и канальном уровне OSI и была предназначена динамического разделения ресурсов физического канала между пользовательскими процессами передачи данных.

Использование технологии FR обеспечивало ряд преимуществ по сравнению с технологиями X.25 и ISDN, которые использовались для обеспечения доступа к распределенным вычислительным ресурсам.

Принципы построения и компоненты сетей Frame Relay

Первоначально информационное взаимодействие технологии FR осуществлялось только на физическом и канальном уровне. В отсутствии сетевого уровня взаимодействия

и заключается принципиальное отличие технологии Frame Relay от ранее существовавших технологий построения сетей. Кадр FR содержит минимум управляющей информации, следствием этого является высокая эффективность передачи данных. Технология Frame Relay не имеет встроенных функций контроля доставки и управления потоком кадров. Предполагается, что каналы передачи данных являются достаточно надежными, а функции управления потоком выполняются протоколами верхних уровней. Эти особенности и обеспечивают преимущества сетей, которые построены по технологии Frame Relay.

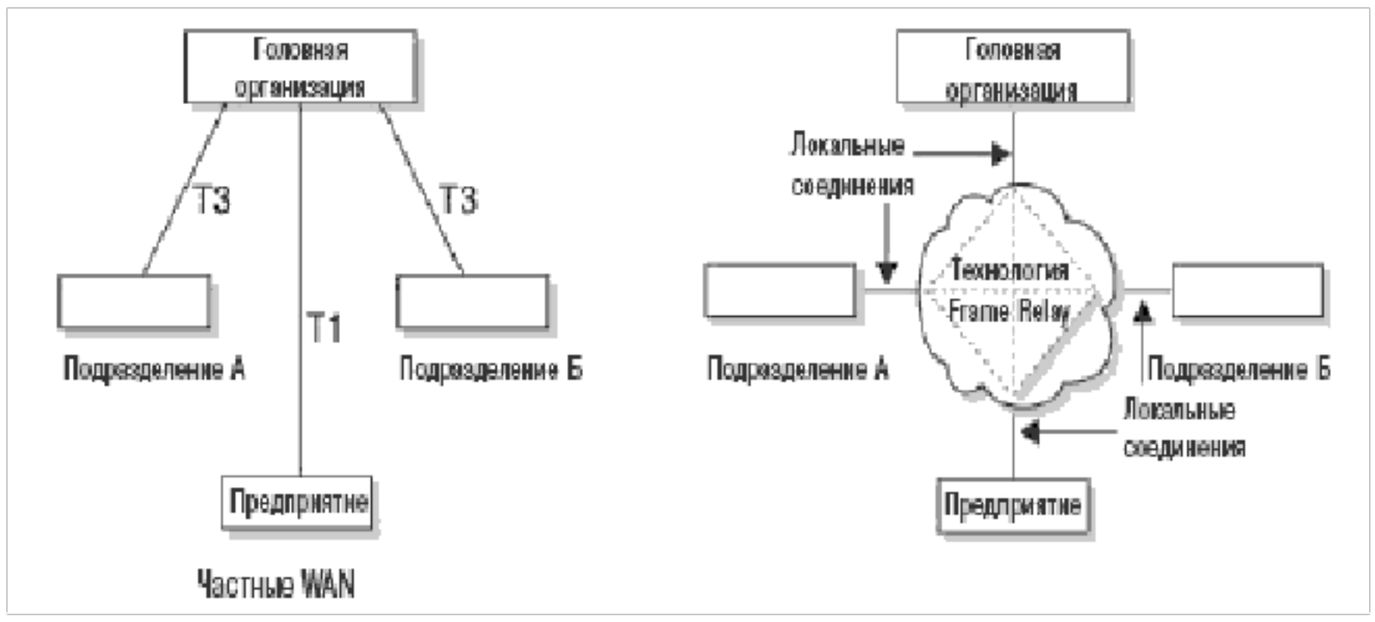


Рисунок 16 - Использование телефонных линий для соединения с удаленными точками

Компонентами сети Frame Relay являются устройства трех основных категорий -
Устройства DTE (Data Terminal Equipment)
Устройства DCE (Data Circuit-Terminating Equipment)
Устройства FRAD (Frame Relay Access Device)

Также как и в сети X.25, основу Frame Relay составляют виртуальные каналы (virtual circuits). Виртуальный канал в сети Frame Relay представляет собой логическое соединение которое создается между двумя устройствами DTE в сети Frame Relay и используется для передачи данных. В сети Frame Relay используется два типа виртуальных каналов — коммутируемые (SVC) и постоянные (PVC).

Технология асинхронного режима передачи (**Asynchronous Transfer Mode, ATM**) отличается от других сетевых технологий тем, что каждая передача состоит из ***53-байтовых ячеек.***

Ячейки - это блоки фиксированной длины и, подобно пакетам, представляют собой части сообщения. Формат фиксированной длины позволяет получать уникальные характеристики:

- *Ориентация на виртуальные каналы связи.* Сетевые соединения, использующие ячейки, наиболее эффективно работают в режиме двухточечного соединения (point-to-point), когда принимающая станция находится в состоянии активности и готова к приему и обработке ячеек.

- *Скорость*. Благодаря одинаковой величине ячеек устройства, обслуживающие технологию АТМ, могут точно определить заголовок ячейки и начало блока данных. Это ускоряет процесс обработки и позволяет АТМ-сетям работать со скоростью до 622 Мбит/с.

- *Качество обслуживания (QoS).* Прогнозируемые скорости передачи данных и виртуальные каналы позволяют гарантировать высокий уровень обслуживания для большей части трафика.

АТМ-технология отличается от технологии Ethernet и Token Ring тем, что является *коммутируемой технологией,* в которой *виртуальные каналы устанавливаются до начала передачи.* Ethernet и Token Ring не создают виртуальных каналов, более того, они отсылают сообщение хосту без предварительного уведомления, оставляя задачу определения оптимального маршрута маршрутизаторам.

Ячейки ATM достаточно малы (53 байта) по сравнению с Ethernet-пакетами, имеющими размер от 64 до 1500 байт, поэтому их быстрее обрабатывать и легче осуществлять контроль.

Технология разработана для оптоволоконных кабелей, работающих в технических условиях синхронных оптических сетей (Synchronous Optical Network, SONET). SONET является ANSI-стандартом, который определяет характеристики физических интерфейсов, подключаемых к оптоволоконным кабелям.

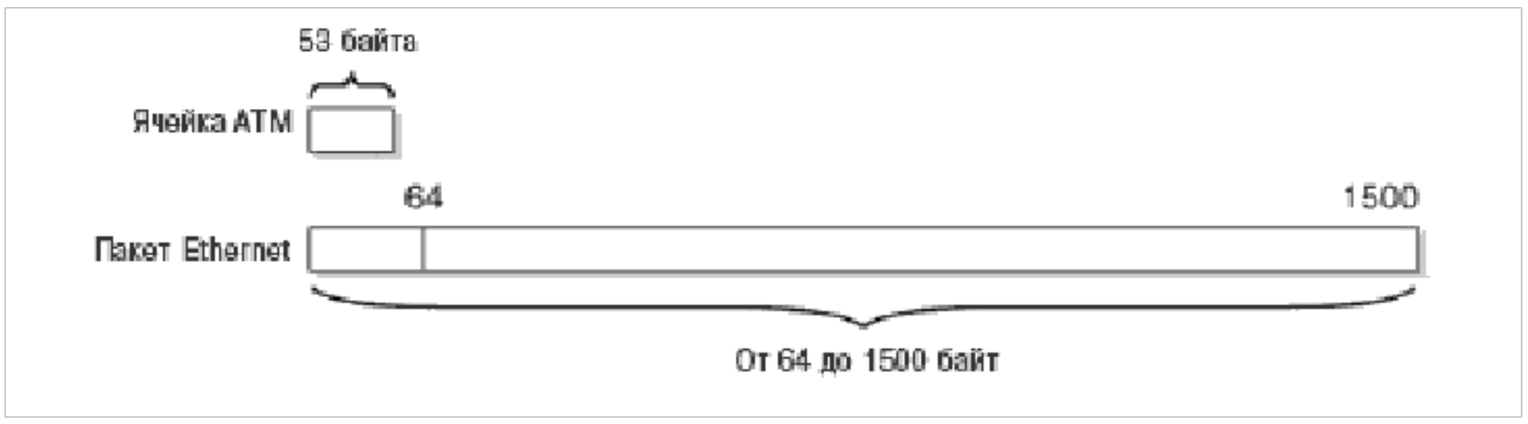


Рисунок 17 – Пример ATM-технологии

Контрольные вопросы

1. Каналы передачи данных, их разновидности. Достоинства, недостатки.
2. Принципы маршрутизации пакетов
3. Преимущества сети с цифровыми каналами передачи данных ISDN
4. Применение технологии ретрансляции кадров Frame Relay
5. Технология ATM

Практическое занятие 14

Беспроводные сети

Цель: ознакомить студентов с технологиями построения беспроводных локальных сетей (WLAN - семейство стандартов 802.11), технологией построения беспроводных сетей городского масштаба (WMax – семейство стандартов 802.16-2004, 802-20, 802-21), и сетей регионального масштаба (WRAN - в рамках стандарта 802.22); требованиями стандартов на Wi Fi (802), WMax (802.16-2004 и др.)

Теоретическая часть:

Беспроводные локальные сети (Wireless LAN, WLAN) "освобождают" устройства от физической привязки к сети, при этом сохраняя возможность передачи данных

Технологической базой для работы беспроводных локальных сетей является стандарт IEEE 802.11.

Протоколы 802.11 и 802.11b работают на частоте 2,4 Гц, а версия 802.11a - на частоте 5,8 Гц.

Рабочая частота 2,4 ГГц - это нелицензированная полоса частот, предназначенная для использования в промышленности, науке и медицине.

Архитектура беспроводных локальных сетей, работающих по стандарту 802.11, напоминает архитектуру сетей сотовой телефонной связи.

Беспроводная локальная сеть (WLAN) 802.11 поделена на ячейки.

- Каждая ячейка управляется ***точкой доступа*** (access point, AP).
- Точка доступа - это устройство, осуществляющее обмен данными с беспроводными сетевыми картами.
- Имеется возможность присоединения множества точек доступа к общей магистрали.
- При совместной работе нескольких AP образуется так называемая **распределенная система (distribution system).**

– Использование архитектуры сотовой связи позволяет беспроводным устройствам соединяться, разъединяться и совершать роуминг от ячейки к ячейке.

Технология WiMAX (описание технологии)

WiMAX- это формат передачи цифровых данных по радиоканалам стандарт 802.16. Это первый стандарт для построения беспроводных сетей масштаба города с радиусом действия свыше 50 км и предоставления абонентам услуг широкополосного беспроводного доступа. При этом передачи сигнала не помешают ни деревья, ни здания, ни особенности местного ландшафта.

WiMAX обеспечивает стабильную работу на высокой скорость передачи данных, - до 300 Мбит/с.

Технология WiMAX обеспечивает широкополосный доступ в тех случаях, когда цифровые линии DSL не могут использоваться по техническим или экономическим причинам. Может применяться операторами голосовой и широкополосной связи для решения проблемы «последней мили», а также для мобильного доступа, дополняющего технологии GSM/Edge, Wi-Fi и 3G.

Плюсы технологии. Решения позволяют развернуть сети широкополосного доступа как на открытой территории площадью в много квадратных километров, так и в здание аэропорта, речного порта, железнодорожного вокзала, центре города, парке, пляже, на набережной, комплекс сооружений и т.п.

Беспроводные сети регионального масштаба (WRAN - в рамках стандарта 802.22).

Новый стандарт, работает на более низких частотах, где ослабление с расстоянием значительно меньше, а препятствия не являются непреодолимой преградой. Новый стандарт IEEE 802.22, работает в диапазоне частот от 54 до 862 МГц.

Данный диапазон частот – имеет следующие уникальные свойства:

– относительно низкий уровень производственных и ионосферных шумов;
– разумные габариты антенн для эффективного приема и передачи сигнала;
– хорошие характеристики распространения сигнала в условиях прямой видимости;
– идеальная возможность для обеспечения больших зон покрытия, особенно в пригороде и сельской местности.

В то же время значительная часть диапазона частот от 54 до 862 МГц активно используется для сетей наземного телевизионного вещания. В этих условиях работа нового стандарта IEEE 802.22 основана на применении когнитивных радиотехнологий, чтобы обеспечить электромагнитную совместимость системы широкополосного радиодоступа и наземного ТВ вещания в одном географическом районе.

Контрольные вопросы

1. Архитектура локальных сетей, работающих по стандарту 802.11
2. Беспроводные сети стандарта 802.22
3. Описание технологии WiMAX.

Практическое занятие 15
Системы управления сетями, объекты и механизмы управления.

Цель: дать студенту основные сведения о протоколе управления SNMP, о принципах распределенного и централизованного администрирования в сетях, о сетевых ПО и операционных системах; описание алгоритма работы протокола управления SNMP, принципы администрирования и мониторинга в сетях; пользоваться стандартами и методами использования технологий администрирования сетями.

Теоретическая часть:

Изучение темы определяет, что одной из основных задач эффективного функционирования сетей является алгоритмы и средства администрирования сети

Простой протокол управления SNMP, включающий минимальный набор команд, однако позволяющий выполнять практически весь спектр задач управления сетевыми устройствами - от получения информации о местонахождении конкретного устройства, до возможности производить его тестирование.

Архитектурная модель SNMP (рисунок 18) представляет собой набор станций сетевого управления и управляемых сетевых элементов. Протокол SNMP используется для обмена информацией между станциями сетевого управления и сетевыми элементами. На станциях сетевого управления выполняются программы, которые обеспечивают мониторинг, и управление сетевыми элементами - так называемые *менеджеры*. В сетевых элементах реализуется *программный агент*.

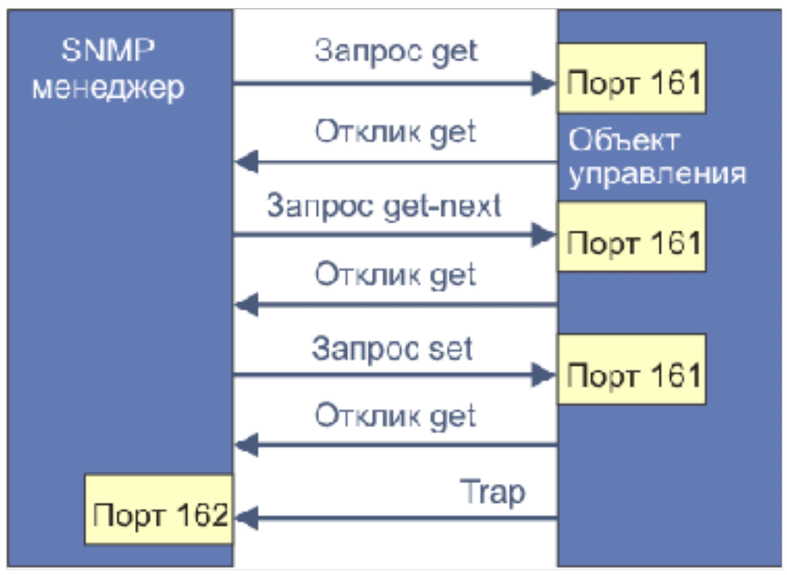


Рисунок 18 - Архитектурная модель SNMP

Протокол SNMP обслуживает передачу данных между агентами и станцией, управляющей сетью. SNMP использует дейтаграммный транспортный протокол UDP, не обеспечивающий надежной доставки сообщений. Протокол, организующий надежную передачу дейтаграмм на основе соединений TCP, весьма загружает управляемые устройства, которые на момент разработки протокола SNMP были не очень мощные, поэтому от услуг протокола TCP решили отказаться.

Протокол SNMP служит основой многих систем управления, хотя имеет несколько принципиальных недостатков, которые перечислены ниже:

1. Отсутствие средств взаимной аутентификации агентов и менеджеров
2. Работа через ненадежный протокол UDP.

Управление сетью связано с применением соответствующих протоколов управления.

В большинстве случаев в сетевом программном обеспечении реализуются протоколы ICMP и SNMP из стека TCP/IP, реже используется протокол CMIP (Common Management Information Protocol) из семиуровневой модели протоколов ISO.

Программное обеспечение управления сетью обычно состоит из **менеджеро**в и **агентов.**

Менеджер называется программа, вырабатывающая сетевые команды.

Агенты представляют собой программы, расположенные в различных узлах сети. Они выполняют команды менеджеров, следят за состоянием узлов, собирают информацию о параметрах их функционирования, сигнализируют о происходящих событиях, фиксируют аномалии, следят за трафиком, осуществляют защиту от вирусов. Агенты с достаточной степенью интеллектуальности могут участвовать в восстановлении информации после сбоев, в корректировке параметров управления и т.п.

ПО сетевых ОС распределено по узлам сети. Имеется ядро ОС, выполняющее большинство из охарактеризованных выше функций, дополнительные программы (службы), ориентированные на реализацию протоколов верхних уровней, выполнение специфических функций для коммутационных серверов, организацию распределенных вычислений и т.п. К сетевому ПО относят также драйверы сетевых плат.

Администрирование сети можно организовать одним из четырех основных способов:

- централизованно на всем предприятии;
- по отделам или группам («распределенное» администрирование);
- по операционным системам;
- в виде сочетания предыдущих способов.

Модели администрирования небольших и крупных, сложных систем могут совпадать. Они будут отличаться масштабами, но не по сути.

Централизованное администрирование

В модели с централизованным администрированием один человек, группа или отдел занимается администрированием всей сети организации, ее пользователей и ресурсов. Главным и очень серьезным недостатком централизованной схемы, является ее недостаточная масштабируемость и отсутствие отказоустойчивости. Производительность центрального компьютера всегда будет ограничителем количества пользователей, работающих с данным приложением, а отказ центрального компьютера приводит к прекращению работы всех пользователей.

Эта модель хорошо подходит небольшим и средним организациям, но может оказаться медленной и неэффективной для крупного или географически разбросанного предприятия. Однако с точки зрения безопасности централизованное администрирование является наилучшим. Оно гарантирует, что системная политика и процедуры являются однообразными для всей организации.

Распределенное администрирование

При распределенном администрировании управление сетью осуществляется на уровне отдела или рабочей группы. Хотя администрирование на этом уровне может быстро откликаться на нужды пользователей, часто это достигается за счет безопасности сети. При наличии нескольких администраторов политика администрирования в разных рабочих группах будет отличаться. Чем больше групп имеется в системе, тем больше доверительных отношений им требуется, что повышает возможность того, что в систему проникнет злоумышленник и воспользуется этими доверительными отношениями, чтобы добраться до совершенно секретной информации.

Администрирование по операционным системам

Когда администрирование домена производится по операционным системам, средства обеспечения безопасности значительно различаются в зависимости от используемых операционных систем. Например, если имеется свой администратор у сервера Windows NT Server, свой — у сервера Novell Net Ware и свой — у систем UNIX, то администратор каждой системы будет сам обеспечивать ее безопасность. Однако потребуется кто-то, кто будет разрешать различия во мнениях администраторов в случае возникновения проблем. В настоящее время наибольшее распространение получили три основные сетевые *ОС - UNIX, Windows NT, Novell Netware*.

Сетевое ПО и операционные системы

Сетевое программное обеспечение (ПО) служит для управления ресурсами всей компьютерной сети.

Основные функции сетевого ПО:

- связывает все компьютеры и периферийные устройства в сети;
- координирует работу всех компьютеров и периферийных устройств в сети;
- обеспечивает защищенный доступ к данным и устройствам в сети.

В состав сетевой ОС входят два основных компонента:

- сетевое ПО компьютеров-клиентов;
- сетевое ПО компьютеров-серверов.

Сетевое ПО компьютеров-клиентов

При автономной работе компьютера запрос на выполнение некоторых действий передается через локальную шину на процессор компьютера. При работе в сетевой среде запрос, относящийся к удаленному серверу, из локальной шины должен быть направлен в сеть и отослан на удаленный сервер.

ПО клиента включает в себя так называемый *редиректор* (redirector), который также может называться *оболочкой* (shell) или *запросчиком* (requester). Переадресация запросов выполняется редиректором.

Редиректор - это небольшая программа сетевой ОС, которая выполняет следующие действия:

• перехватывает запросы в компьютере;

• определяет куда следует направить запрос: на локальную шину или в сеть для пересылки на удаленный сервер.

• посылает запрос как к компьютерам, так и к сетевым периферийным устройствам.

Сетевое ПО компьютеров-серверов

Серверное ПО обеспечивает совместное использование ресурсов и координирует различные уровни доступа. Оно дает возможность всем сетевым компьютерам совместно использовать данные сервера и его периферийные устройства.

В современных сетевых операционных системах автономная и сетевая ОС скомбинированы в одну ОС, которая поддерживает функционирование, как автономного компьютера, так и целой сети. Например, по этому принципу построена сетевая ОС Windows NT Server.

Администратор сети, через сервер, управляет и пользователями и сетью.

Сетевые операционные системы

Под сетевой операционной системой в широком смысле понимается совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам - протоколам. В узком смысле сетевая ОС - это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.

В сетевой операционной системе отдельной машины можно выделить несколько частей:

• *Средства управления локальными ресурсами компьютера*:

– функции распределения оперативной памяти между процессами,

– планирования и диспетчеризации процессов,

– управления процессорами в мультипроцессорных машинах,

– управления периферийными устройствами и

– другие функции управления ресурсами локальных ОС.

• *Средства предоставления собственных ресурсов и услуг в общее пользование - серверная часть ОС (сервер):*

– блокировку файлов и записей;

– ведение справочников имен сетевых ресурсов;

– обработку запросов удаленного доступа к собственной файловой системе и базе данных;

– управление очередями запросов удаленных пользователей к своим периферийным устройствам.

• *Средства запроса доступа к удаленным ресурсам и услугам и их использования - клиентская часть ОС (редиректор).*

Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей, при этом запрос поступает от приложения в локальной форме, а передается в сеть в другой форме, соответствующей требованиям сервера. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.

• *Коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети.*

Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи и т.п., то есть является средством транспортировки сообщений.

Контрольные вопросы

1. Функции протокола управления SNMP

2. Назначение программ *менеджер* и *агент*

3. Способы администрирования сети. Сравнение моделей централизованного и распределенного администрирования.

4. Основные функции сетевого ПО. Что понимается под понятием *сетевая ОС*.

5. Функции *редиректора*

6. Принцип построения сетевой ОС Windows NT Server

7. Коммуникационные средства ОС

Практическое занятие 16
Безопасность и защита данных.

Цель: дать студенту основные сведения об обеспечении безопасности данных в сетях; модель архитектуры защиты, методы защиты (аутентификация, управление доступом, конфиденциальность, целостность данных), распределение услуг защиты по уровням.

Теоретическая часть:

Решение проблем защиты данных в сетях важнейшая задача пользователей.

Основными угрозами безопасности информации, являются следующие:

- увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
- сосредоточение в единых базах данных информации различного назначения и различной принадлежности;
- расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней массивам данных;
- усложнение режимов работы технических средств вычислительных систем;
- автоматизация межмашинного обмена информацией, в том числе на больших расстояниях;
- слабая подготовка (недостаточная квалификация) персонала.

Все угрозы безопасности информации можно классифицировать по следующим признакам:

- по цели воздействия;
- по характеру воздействия и
- по способу возникновения

В зависимости от характера воздействия нарушителя могут быть выделены активные и пассивные угрозы безопасности информации.

- При пассивном вторжении (перехвате информации) нарушитель только наблюдает за прохождением информации в ВС, не вторгаясь ни в информационный поток, ни в содержание передаваемой информации.

При активном вторжении нарушитель стремится изменить информацию, передаваемую в сообщении.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ (НСД). Суть НСД состоит в получении нарушителем доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой политикой безопасности. НСД может быть осуществлен как штатными средствами системы, так и специально созданными аппаратными и программными средствами.

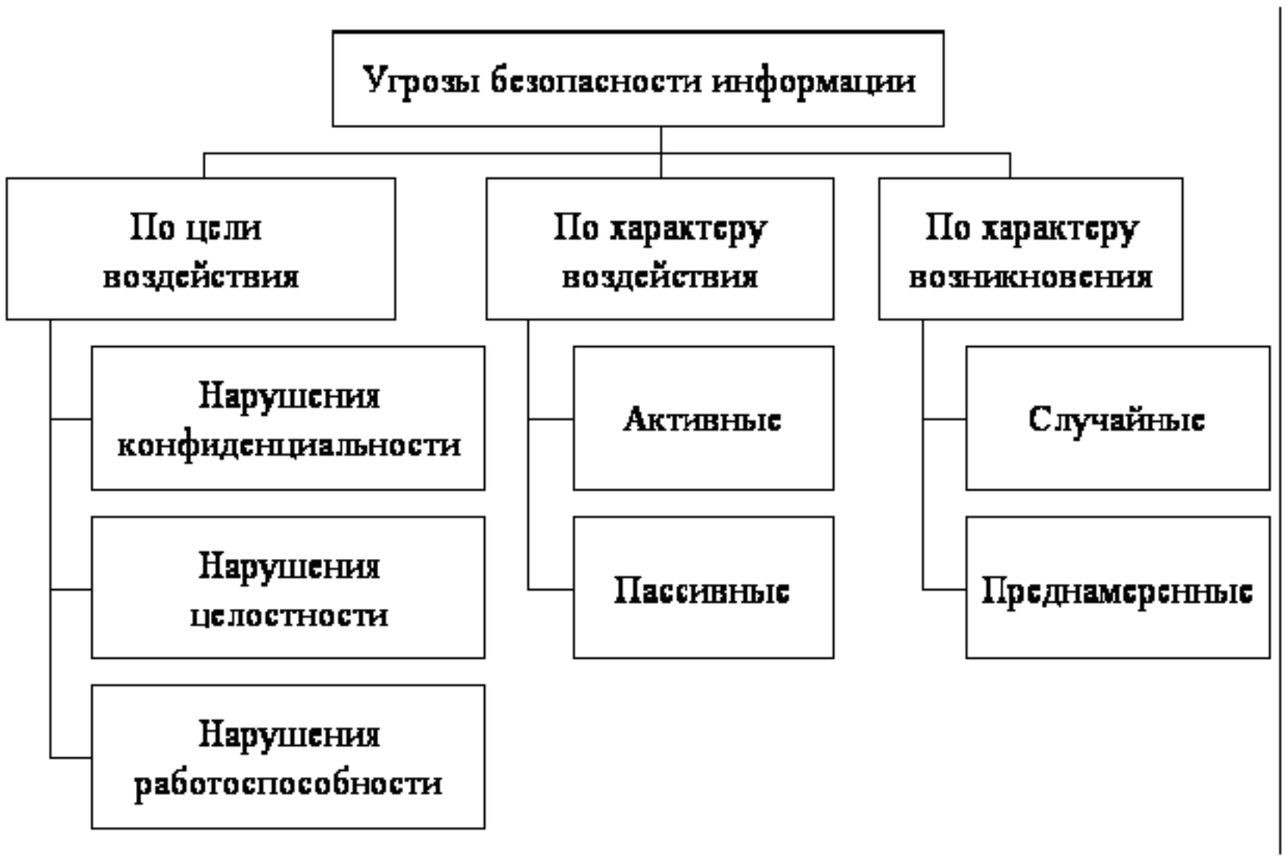


Рисунок 1 – угрозы безопасности информации

Существующие подходы к повышению уровня защищенности вычислительных сетей.

• Главным направлением в данной предметной области следует считать развитие рецепторных схем выявления несанкционированных действий, позволяющих использовать активные средства защиты в виде параметрической или структурной адаптации с целью увеличения параметра .

• Системы обнаружения атак создаются, чтобы обеспечить дополнительный уровень защиты вычислительной сети, дополняя традиционные средства защиты: межсетевые экраны, криптомаршрутизаторы, серверы аутентификации и т. д. Очень часто противник в первую очередь атакует и пытается вывести из строя, имеющиеся защитные средства, обеспечивающие безопасность выбранной им цели.

• Обнаруживать, блокировать и предотвращать нарушения политики безопасности можно несколькими путями. Первый и самый распространенный способ – это распознавание уже реализуемых атак. Это способ применяется в классических системах обнаружения атак. Однако недостаток средств данного класса в том, что атаки могут быть реализованы повторно.

• Поэтому было бы правильнее предотвращать атаки еще до их осуществления. В этом и заключается суть второго способа. Реализуется он путем поиска уязвимостей, которые могут быть использованы для совершения атаки. И, наконец, третий путь – выявление уже совершенных атак и предотвращение их повторения в дальнейшем.

Реализация политики защиты средствами **транспортного уровня** осуществляется с помощью межсетевых экранов (firewall). Межсетевой экран — это специализированное программное обеспечение, реализующее фильтрацию трафика в соответствии с правилами политики защиты сети средствами транспортного уровня. Как правило, данное программное обеспечение функционирует на платформе маршрутизатора, управляющего информационными потоками узлов различных сетей.

На сетевом уровне OSI решение проблемы защиты очевидно — нужно использовать все адресное пространство и не дать злоумышленнику возможности захватить адреса неиспользуемых узлов. Одним из способов является применение службы мониторинга сети и поддержки виртуальных узлов в резервном диапазоне адресов. Данная служба постоянно использует свободное адресное пространство сети, создавая собственные виртуальные хосты (новые виртуальные хосты создаются сразу после отключения от сети реально функционирующих доверенных узлов). Таким образом, служба **подменяет собой** отсутствующие в настоящий момент рабочие станции, серверы, маршрутизаторы и т.д.

Обеспечение безопасности разделения среды передачи коммуникационными средствами **канального уровня**. Протоколы и стандарты этого уровня описывают процедуры проверки доступности среды передачи и корректности передачи данных.

Средства коммутации канального уровня, используемые в компьютерной сети предприятия, должны быть настраиваемыми и обеспечивать разграничение доступа между узлами сети в соответствии с разработанной политикой. Как правило, такие средства поддерживают технологию VLAN, позволяющую в рамках одного коммутатора выделить группы аппаратных адресов и сформировать для них правила трансляции кадров.

Администратор сети должен выполнить настройку подсистемы управления VLAN коммутатора, и других подсистем, необходимых для реализации разработанной политики защиты. В обязанности администратора входит также отключение неиспользуемых подсистем коммутатора.

Администратор сети должен регулярно контролировать соответствие конфигураций коммутаторов разработанной политике защиты.

Администратор сети должен вести мониторинг сетевой активности пользователей с целью выявления источников аномально высокого количества широковещательных запросов.

Служба безопасности должна контролировать регулярность смены реквизитов авторизации администратора в подсистемах управления коммутаторами.

Служба безопасности должна контролировать регулярность выполнения администратором мероприятий, связанных с мониторингом сети, осуществлением профилактических работ по настройке коммутаторов, а также созданием резервных копий конфигураций коммутаторов.

Служба безопасности должна обеспечить строгий контроль доступа в помещения, в которых расположены коммутаторы и рабочие станции, с которых разрешено управление коммутаторами.

Контрольные вопросы

1. Факторы, способствующие информационной уязвимости
2. Классификация угроз безопасности информации по признакам
3. Активное и пассивное вторжение
4. Подходы к повышению уровня защищенности вычислительных сетей
5. Решение проблемы защиты на канальном, сетевом, транспортном уровнях OSI

Практическое занятие 17
Принципы построения Internet

Цель: дать студенту основные сведения об организации Internet, о представлении информации в Internet, о серверах и протоколах Internet, о языках HTML и XML; организацию взаимосвязей между документами (гиперссылки), принципы создания WEB-страниц; создавать WEB-страницы

изучение Темы необходима для активного использования сервисов Интернет, создания собственных WEB-страницы и т.п.

Теоретическая часть:

Internet – всемирная информационная компьютерная сеть, представляющая собой объединение множества региональных компьютерных сетей и компьютеров, обменивающих друг с другом информацией по каналам общественных телекоммуникаций (выделенным телефонным аналоговым и цифровым линиям, оптическим каналам связи и радиоканалам, в том числе спутниковым линиям связи).

Информация в Internet хранится на серверах. Серверы имеют свои адреса и управляются специализированными программами. Они позволяют пересылать почту и файлы, производить поиск в базах данных и выполнять другие задачи.

Обмен информацией между серверами сети выполняется по высокоскоростным каналам связи (выделенным телефонным линиям, оптоволоконным и спутниковым

каналам связи). Доступ отдельных пользователей к информационным ресурсам Internet обычно осуществляется через провайдера или корпоративную сеть.

Провайдер - поставщик сетевых услуг – лицо или организация предоставляющие услуги по подключению к компьютерным сетям. В качестве провайдера выступает некоторая организация, имеющая модемный пул для соединения с клиентами и выхода во всемирную сеть.

Основными ячейками глобальной сети являются локальные вычислительные сети. Если некоторая локальная сеть непосредственно подключена к глобальной, то и каждая рабочая станция этой сети может быть подключена к ней.

Существуют также компьютеры, которые непосредственно подключены к глобальной сети. Они называются хост - компьютерами (host - хозяин). Хост – это любой компьютер, являющийся постоянной частью Internet, т.е. соединенный по Internet – протоколу с другим хостом, который в свою очередь, соединен с другим, и так далее.

Практически все услуги Internet построены на принципе клиент-сервер. Вся информация в Интернет хранится на серверах. Обмен информацией между серверами осуществляется по высокоскоростным каналам связи или магистралям. Серверы, объединенные высокоскоростными магистралями, составляют базовую часть сети Интернет.

Отдельные пользователи подключаются к сети через компьютеры местных поставщиков услуг Интернета, Internet - провайдеров (Internet Service Provider - ISP), которые имеют постоянное подключение к Интернет. Региональный провайдер, подключается к более крупному провайдеру национального масштаба, имеющего узлы в различных городах страны. Сети национальных провайдеров объединяются в сети транснациональных провайдеров или провайдеров первого уровня. Объединенные сети провайдеров первого уровня составляют глобальную сеть Internet.

Передача информации в Интернет обеспечивается благодаря тому, что каждый компьютер в сети имеет уникальный адрес (IP-адрес), а сетевые протоколы обеспечивают взаимодействие разнотипных компьютеров, работающих под управлением различных операционных систем.

В основном в Интернет используется семейство сетевых протоколов (стек) TCP/IP. На канальном и физическом уровне стек TCP/IP поддерживает технологию Ethernet, FDDI и другие технологии. Основой семейства протоколов TCP/IP является сетевой уровень, представленный протоколом IP, а также различными протоколами маршрутизации. Этот уровень обеспечивает перемещение пакетов в сети и управляет их машрутизацией. Размер пакета, параметры передачи, контроль целостности осуществляется на транспортном уровне TCP.

Прикладной уровень объединяет все службы, которые система предоставляет пользователю. К основным прикладным протоколам относятся: протокол удаленного доступа telnet, протокол передачи файлов FTP, протокол передачи гипертекста HTTP, протоколы электронной почты: SMTP, POP, IMAP, MIME.

По способу представления информации источники можно разделить на несколько основных категорий:

Web-страницы – это основной и наиболее распространенный тип информационных ресурсов в Сети. Они представляет собой страницы так называемого гипертекста, то есть текста, который может содержать в себе ссылки. Совокупность гипертекстовых страниц, расположенная в одном месте, представляет собой единицу, называемую САЙТОМ.

Gopher является другим гипертекстовым стандартом, практически не развивающимся сегодня, поскольку поддерживает только текстовую форму представления информации. Однако это не мешает стандартнм броузерам понимать и этот формат.

Базы данных также могут иметь быть доступны через Сеть. Базы данных могут содержать произвольную информацию. В настоящий момент не существует какого-либо стандартного способа доступа к базам данных по сети Интернет. Наиболее часто пользуются доступом к базам данных через стандартные броузеры.

Файловые серверы - это традиционный способом хранения данных в Интернете. Они представляют собой компьютеры. Часть их дискового пространства доступна по Сети. Доступ к данным на таком сервере осуществляется с помощью специальных программ, поддерживающих протокол передачи файлов (FTP - File Transfer Protocol).

Данный протокол идентификации пользователя, запросившего доступ к данным. Для осуществления доступа к файлам со стороны произвольного пользователя Сети обычно используется анонимный вход (anonymous).

Этот протокол обычно поддерживается стандартными броузерами.

Телеконференции также могут являться источником необходимой информации, как правило, носящей неофициальный характер. Телеконференции представляют собой способ общения людей, имеющих доступ в Сеть, и предназначены для обсуждения каких-либо вопросов или распространения информации. Все телеконференции разбиты по тематическому признаку на рубрики, иначе называемые группами новостей (news groups). Информация, помещенная в телеконференцию, становится на определенное время доступна всем желающим.

Протокол передачи гипертекста HTTP

Служба *WWW,* как и любая иная сетевая служба, строится на взаимодействии пары программ: сервера и клиента. Программы-серверы *WWW* называются *Web-серверами* - они работают на компьютерах, которые называются *сетевыми серверами.* В общем, одно и то же слово *сервер,* в зависимости от контекста, может обозначать то ли компьютер, то ли программу.

Программы-клиенты WWW называются *Web-браузерами* — они работают на наших с вами клиентских компьютерах. Взаимодействие между Web-сервером и Web-браузером происходит по специальному прикладному протоколу —*HTTP (HypertextTransferProtocol,* протокол передачи гипертекста). Несмотря на столь длинное и страшное название, протокол *HTTP* чрезвычайно прост — это один из самых простых прикладных протоколов Интернета. Суть его в том, что браузер имеет право обратиться к серверу с запросом, в котором указан *URL-адрес* требуемого ресурса. Это может быть Web-страница, рисунок, программный объект и т. п. Сервер передает браузеру затребованный ресурс, после чего соединение разрывается до следующего запроса.

XML - это расширяемый язык разметки (Extensible Markup Language), разработанный специально для размещения информации в World Wide Web, наряду с HTML, который давно стал стандартным языком создания Web-страниц. В отличие от HTML, вместо использования ограниченного набора определённых элементов вы имеете возможность создавать ваши собственные элементы и присваивать им любые имена по вашему выбору. Примечание: подразумевается, что читатель данной статьи хотя бы очень поверхностно знаком с языком HTML.

XML решает ряд проблем, которые не решает HTML, например:

- Представление документов любого (не только текстового) типа, например, музыки, математических уравнений и т.д.
- Сортировка, фильтрация и поиск информации.
- Представление информации в структурированном (иерархическом) виде.

В зависимости от уровня соответствия стандартам документ может быть "верно сформированным" ("well-formed"), либо "валидным" ("valid"). Вот несколько основных правил создания верно сформированного документа:

- Каждый элемент XML должен содержать начальный и конечный тэг (либо пустой тэг типа <TAG />, который может нести информацию посредством своих атрибутов).
- Любой вложенный элемент должен быть полностью определён внутри элемента, в состав которого он входит.
- Документ должен иметь только один элемент верхнего уровня.
- Имена элементов чувствительны к регистру.

Есть три основных способа сообщить браузеру, как отображать каждый из созданных вами XML-элементов:

• Каскадная таблица стилей (Cascading Style Sheet - CSS) или расширяемая таблица в формате языка стилевых таблиц (Extensible Stylesheet Language - XSL).

• Связывание данных. Этот метод требует создания HTML-страницы, связывания с ней XML-документа и установления взаимодействий HTML-элементов с элементами XML. В дальнейшем HTML-элементы автоматически отображают информацию из связанных с ними XML-элементов.

• Написание сценария. Этот метод требует создания HTML-страницы, связывания с ней XML-документа и получение доступа к XML-элементам с помощью кода сценария JavaScript или VBScript.

XML-приложение обычно определяется созданием описателя типа документа (DTD), который является допустимым компонентом XML-документа. DTD устанавливает и определяет имена элементов, которые могут быть использованы в документе, порядок, в котором элементы могут появляться, и доступные к применению атрибуты элементов. DTD обычно включается в XML-документ и ограничивает круг элементов и структур, которые будут использоваться. Примечание: приложение XML Schema позволяет разрабатывать подробные схемы для ваших XML-документов с использованием стандартного синтаксиса XML и является альтернативой DTD.

Языки **HTML** и **XML** предназначены для решения разных задач. Учитывая прекрасную структуру XML и место, реально занимаемое HTML в практике Web-дизайна, было решено объединить HTML и XML. В результате появился XHTML. Появление XHTML означает, что HTML переопределяется как приложение XML. Отныне HTML должен подчиняться правилам XML.

В настоящее время заметно растет интерес к улучшению того, что представлено в Web-браузерах и альтернативных устройствах. Идеология HTML 4.0, перенесенная в XHTML 1.0, переходит в концепцию разработки документов для разных типов устройств.

В версии XHTML 1.0 обязательно строгое соблюдение правил разметки, что способствует улучшению структуры и синтаксиса разметки. Это чрезвычайно важно, так как в настоящее время Web интенсивно выходит за рамки браузеров. Будущий информационный дизайнер должен будет учитывать в своих разработках многочисленные альтернативные пользовательские устройства. Документы должны быть логичными и эстетически привлекательными в таких средах, как пейджеры, PDA (Personal Digital Assistant - персональный цифровой помощник), сотовые телефоны и т.д.

С помощью тегов *HTML*можно связать любой элемент Web-страницы (например, текст или рисунок) с каким-либо адресом *URL*. Такие связи называются *гиперссылками*. При просмотре Web-страницы в браузере текстовые гиперссылки выделяются, синим цветом и подчеркиванием (если используется стандартная настройка). При щелчке левой кнопкой мыши на гиперссылке происходит загрузка другого Web-документа — того, на который указывает адрес *URL*, записанный в этой гиперссылке.

Благодаря гипертекстовым связям все пространство WWW можно рассматривать как единую паутину, состоящую из множества взаимосвязанных документов. Сегодня в этой паутине насчитывается более пяти миллиардов документов, и их число очень быстро растет. Теоретически, начав работу в *WWW* с просмотра одного-единственного документа, можно бесконечно блуждать в паутине, получая все новую и новую информацию. Приемы навигации в *WWW*— это отдельная тема для обстоятельного обсуждения. Навигация — еще одна из функций Web-браузеров.

Клиентский *скрипт* - это программа, которая может сопровождать документ HTML или непосредственно быть внедренной в него. Эта программа выполняется на клиентской машине при загрузке документа или в другое время, например, когда активизируется ссылка. Поддержка скриптов в HTML не зависит от языка скрипта.

Скрипты предлагают авторам средства усиления интерактивности документов HTML. Например:

• Скрипты могут оцениваться во время загрузки документа и динамически изменять содержимое документа.

• Скрипты могут использоваться в форме для обработки вводимых данных. Дизайнеры могут динамически заполнять поля формы в зависимости от значений других полей. Они могут проверять, попадают ли введенные данные в предопределенный диапазон значений, соответствие полей и т.д.

• Скрипты могут включаться событиями, оказывающими влияние на документ, например, загрузкой, выгрузкой, фокусом элемента, перемещением мыши и т.д.

• Скрипты могут связываться с управляющими элементами формы (например, с кнопками) для представления элементов пользовательского интерфейса.

Авторы могут прикреплять к документу HTML два типа скриптов:

• Скрипты, выполняющиеся один раз при загрузке документа агентом пользователя. Скрипты, описанные в элементе SCRIPT, выполняются при загрузке документа. Для агентов пользователя, не обрабатывающих скрипты, авторы могут определить альтернативное содержимое с помощью элемента NOSCRIPT.

• Скрипты, выполняемые каждый раз, когда происходит определенное событие. Эти скрипты могут назначаться ряду элементов с помощью атрибутов внутренних событий

Для расширений функций web-сервера приходится разрабатывать специальные программы, называемые **расширениями web-сервера** или **web-приложениями**. Существует много типов web-приложений. Одним из таких типов расширений являются **CGI** (CommonGateInterface) **приложения**, в основе которых лежит использование общего шлюзового интерфейса. Такие приложения подчиняются правилам передачи информации по протоколу HTTP. CGI-приложение получает в соответствии с протоколом HTTP информацию от пользователя, обрабатывает её и возвращает результат обработки в виде HTML-документа, созданного динамически или в виде ссылки на уже существующий документ или другой объект, например, графическое изображение. Отображаемый на экране клиентского компьютера результат называют **web-страницей**. CGI - это первый общепринятый интерфейс, считающийся классическим для создания расширений web-серверов. CGI-приложения представляют собой обычное консольное приложение, которое обменивается данными с web-сервером через так называемое переменное окружение выполняющейся программы (параметры).

Недостатки CGI:

Приложение выполняется в своем адресном пространстве, поэтому скорость его взаимодействия с web-сервером невысока;

Осуществлять обмен данными через переменное окружение достаточно неудобно.

Тем не менее, до сих пор широко распространен из-за универсальности (подходит под все известные ОС).

Передача информации от пользователя, работающего на клиентском компьютере, CGI-приложению и обратно выполняется обычно так:

1) в HTML-документе, который создается для ввода информации, предназначенной для обработки, размещается форма ввода. Эта форма состоит из необходимых элементов управления, подобных тем, которые используются в приложениях, разрабатываемых с использованием системы Builder(Delphi). Каждому элементу управления присваивается имя, используемое для ссылки на элемент управления и для идентификации значений атрибутов элементов. Кроме того, в этой форме предусматривается кнопка, которую следует нажать после заполнения формы. Когда пользователь заполняет форму и нажимает указанную кнопку, данные передаются CGI-приложению, местонахождение которого задается в описании формы.

2) CGI-приложение получает согласно протоколу HTTP данные из элементов формы в виде пар: имя элемента - значение.

3) После обработки полученных данных CGI-приложение создает HTML-документ и помещает его в стандартный поток вывода. Этот сформированный HTML-документ затем автоматически передается web-сервером пользователю и отображается как web-страница на клиентском компьютере.

Контрольные вопросы

1. Протоколы обмена, используемые в Internet
2. Функции протоколов TCP и IP
3. Прикладной протокол — HTTP
4. Принципы построения услуг Internet
5. Способы хранения данных в Internet
6. Принципы рганизации WEB-страниц

Практическое занятие 18
Web-узлы.

Цель: дать студенту основные сведения о Web-узлах, browser-программах, сайтах, координационных группах, провайдерах. WEB-серверах. DNS – службе; способах организации Web-узла, использования Браузер – программы, основные и дополнительные функции веб-сервера.

Теоретическая часть:

Понимание Web-технологий позволяет пользователю эффективно использовать Интернет в своей деятельности во всех сферах.

Web-узлы, browser-программы, сайты, координационные группы, провайдеры. WEB-серверы. DNS – служба.

Web-узлы (сайт) - это наборы связанных Web-страниц, размещенных в одном домене. Узлы обычно посвящаются какой-то определенной теме, например, обмену мнениями по поводу проблем создания Web-страниц, различным видам развлечений и т. д.

Web-узлы могут также включать связи с другими узлами. Все это и приводит к созданию информационной всемирной "паутины".

Первый документ Web-узла называется начальной (или основной) страницей (home page). Начальная страница содержит ссылки на все остальные документы второго уровня. Так как связи между страницами могут быть очень сложными Web-дизайнеры пользуются картами узла, чтобы разобраться во всех возможных путях следования.

На каждой Web-странице следует располагать не более 10 ссылок на страницы, с которыми она непосредственно связана. Большее количество ссылок плохо воспринимается пользователем; кроме того, дизайнеру тоже сложно работать с таким громоздким документом.

Web-узел с большим количеством страниц должен быть организован более сложно. Связи между страницами разных уровней повторяются, при этом создается карта узла, которая выглядит примерно как генеалогическое дерево. Web -узел, содержащий более 10 документов, может быть организован по трем уровням.
В таком случае каждая страница второго уровня является дочерней по отношению к начальной странице и родительской для страниц третьего уровня, которые с ней связаны. Этот принцип можно повторять для четырех, пяти или более уровней, в зависимости от числа документов на узле.

Создание Web-узла — это достаточно трудоемкий процесс, требующий не только больших затрат времени, но и обширных знаний в области разработки. Программа FrontPage идет навстречу разработчикам, предоставляя в их распоряжение средства, призванные сократить до минимума время, затрачиваемое на создание проекта. Среди них большое количество шаблонов и мастеров по созданию Web-страниц, фреймов, Web-узлов и стилей.

Браузер – программа установленная на каждом компьютере имеющем доступ в сеть интернет.

При помощи браузеров вы получаете возможность просматривать интернет странички и быть полноценным пользователем сети. Стандартный, поставляемые с системой браузеры, на сегодняшний день имеют замечательные бесплатные альтернативы, которые можно скачать.

Новая версия браузера **Opera 11.00.1055a Portable** поддерживает виджеты-расширения (extensions). С помощью этих модулей, которые встраиваются в браузер, пользователи могут получить доступ к различному функционалу, который недоступен в стандартной версии Opera. Данная сборка включает в себя последнюю версию браузера Opera и полный комплект плагинов, необходимых для комфортного серфинга в интернете (использовалась сборка Plugins for Opera и AntiBanner for Opera). Также настроен анти-баннер, который предотвращает загрузку так надоевших всем рекламных блоков (баннеров) на сайтах и блокирует всплывающие рекламные окна (popup и clickunder)! Opera – один из самых быстрых и гибких в настройке браузеров. Дополнительно оптимизированный механизм обработки javascript стал быстрее.

Google Chrome - веб-браузер производства Google с открытым исходным кодом, сочетающий поддержку новейших веб-приложений и удобный поиск с высокой скоростью и стабильностью. Из особенностей Chrome разработчики особенно выделяют изолированные вкладки, предотвращающие сбой работы программы и обеспечивающие более надежную защиту от опасных сайтов.

Веб-сервер (web-server) - это сервер, отвечающий за прием и обработку запросов (HTTP-запросов) от клиентов к веб-сайту. В качестве клиентов обычно выступают различные веб-браузеры. В ответ веб-сервер выдает клиентам HTTP-ответы, в большинстве случаев, вместе с HTML-страницей, которая может содержать: всевозможные файлы, какие-то изображения, медиа-поток или любые другие данные.

Также веб-сервер выполняет исполнение скриптов, например, таких как CGI, JSP, ASP и PHP, которые отвечают за организацию запросов к сетевым службам, базам данных, доступу к файлам, пересылке электронной почты и другим приложениям электронной коммерции.

Термин Веб-сервер также применяется к техническим устройствам и программному обеспечению, которые выполняет функции веб-сервера. Это может быть какой-нибудь компьютер, который специально выделен из группы персональных компьютеров или рабочая станция, на которых установлено и работает сервисное программное обеспечение.

Клиент пользователя, которым преимущественно является веб-браузер, передает веб-серверу запросы на получение ресурсов, обозначенных URL-адресами. Ресурсы - это HTML-страницы, цифровой медиа контент, медиа-потоки, различные изображения, файлы данных, или любые другие данные, необходимые клиенту. В ответ веб-сервер передает клиенту запрошенные им данные. Этот обмен происходит с помощью протокола HTTP.

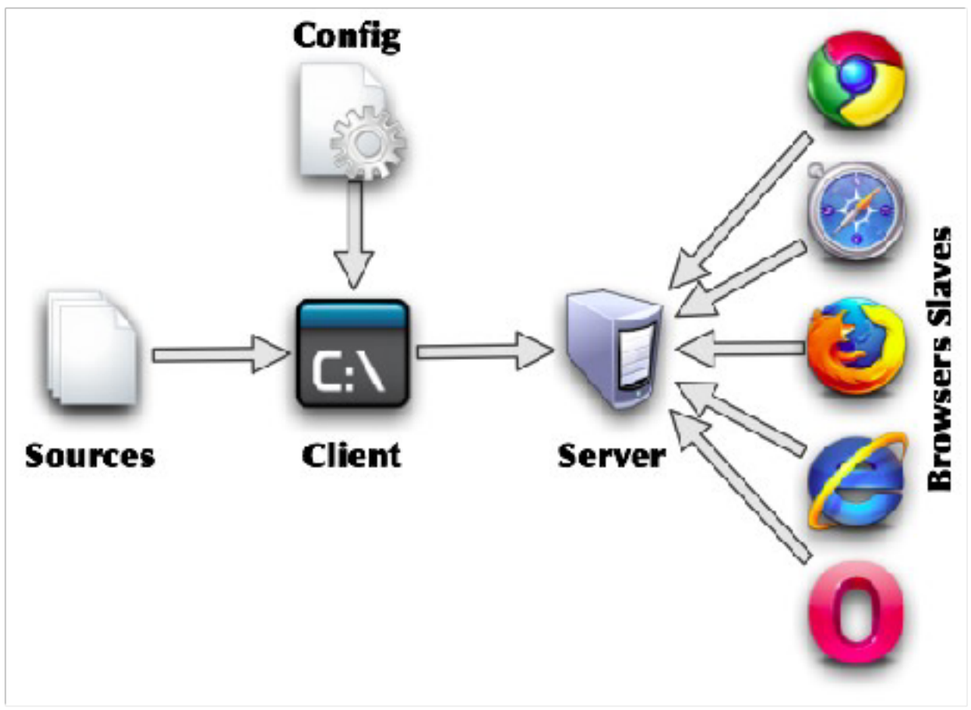
HTTP (англ. HyperText Transfer Protocol - протокол передачи гипертекста) – это сетевой протокол прикладного уровня передачи данных. Основным принципом протокола HTTP является технология «клиент-сервер», обеспечивающая взаимодействие сети и пользователя.

В случае малой организации веб-сервер может быть целостной системой, которая будет состоять из: HTTP-сервера – служит для запросов к веб-страницам, FTP-сервера – применяется для загрузки файлов через Интернет, NNTP-сервера – выполняет доступ к группам новостей, а также SMTP-сервера - для электронной почты.

Основные и дополнительные функции веб-сервера:

- Прием запросов от веб-браузеров по протоколу стандарта HTTP с использованием сетевых протоколов TCP/IP;
- Выполнение поиска и отсылки файлов с гипертекстом или каких-либо документов в браузер по протоколу HTTP;

- Обслуживание и обработка запросов, типа: mailto:..., FTP, Telnet и т.п.
- Запуск прикладных программ на веб-сервере с последующей передачей и возвратом параметров обработки через стандарт интерфейса CGI;
- Работа и обслуживание навигационных карт изображений (Image map);
- Загрузка Java-приложений;
- Администрация и оперативное управление сервером;
- Авторизация пользователей и их аутентификация;
- Ведение регистрационного журнала обращений пользователей к различным ресурсам;
- Автоматизированная работа веб-страниц;
- Поддержка страниц, которые генерируются динамически;
- Поддержка работы протокола HTTPS для защищенных соединений с клиентами.



Веб-браузеры поддерживают связь с веб-серверами с помощью протокола передачи гипертекстовых сообщений (HypertextTransferProtocol, HTTP). Это простой протокол запросов и ответов для пересылки информации с использованием протокола TCP/IP. Веб-сервер получает запрос, обнаруживает файл, посылает его браузеру, а затем разрывает соединение. Графическая информация, которая имеется на странице, обрабатывается таким же образом. Далее настает очередь веб-браузера вывести на монитор пользователя, загруженный из сети HTML-документ.

Кроме HTML-страниц и графики, веб-серверы могут хранить любые файлы, в том числе текстовые, документы текстовых процессоров, видеофайлы и аудиоинформацию. На сегодняшний день, если не учитывать анкет, которые заполняют пользователи, основная часть веб-трафика передается в одном направлении - браузеры считывают файлы с веб-сервера. Но это положение изменится после общего принятия описанного в проекте HTTP 1.1 метода PUT, который позволяет записывать файлы на веб-сервер. Сегодня метод PUT используется в основном пользователями, создающими веб-страницы, но в перспективе он может пригодиться и остальным пользователям для обратной связи с информационными центрами. Запросы методом PUT намного проще, чем обыкновенная POST загрузка файлов на веб-сервер.

На веб-сервере также выполняют свою работу различные приложения, наибольшую популярность среди которых, получили поисковики и средства связи с базами данных. Для разработки этих приложений применяются такие стандарты, как общий шлюзовой интерфейс (CommonGatewayInterface, CGI), языки сценариев JavaScript, а также языки программирования Java и VisualBasic. Кроме интерфейса стандарта CGI, некоторые фирмы-разработчики веб-серверов создали интерфейсы прикладного программирования (API) такие как, например, Netscape Server API и Internet Server API, которые созданы компаниями Microsoft и Process Software AG. Эти интерфейсы позволяют разработчикам непосредственно обращаться к конкретным функциям веб-сервера. Некоторые веб-серверы обладают связующим

программным обеспечением (middleware) для подключения к базам данных, работа с которыми может потребовать профессиональных знаний в программировании.

DNS – служба.

Служба доменных имен (DNS) - это протокол разрешения имен для сетей TCP/IP, таких как Интернет. DNS-сервер содержит сведения, с помощью которых клиентские компьютеры могут разрешать легко запоминающиеся буквенно-цифровые DNS-имена в IP-адреса, используемые компьютерами для связи друг с другом.

Контрольные вопросы

1. Разница между Web-узлами и Web-страницами
2. Браузер – программа
3. Функции веб-сервера
4. Протоколом, обеспечивающий связь веб-браузера с веб-серверами
5. Принцип организации DNS – службы

Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

5.1.1. Перечень основной литературы:

1. Берлин А.Н. Телекоммуникационные сети и устройства [Электронный ресурс]/ Берлин А.Н.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 395 c.— Режим доступа: http://www.iprbookshop.ru/52197.— ЭБС «IPRbooks», по паролю

2. Зиангирова Л.Ф. Вычислительные системы, сети и телекоммуникации [Электронный ресурс]: учебно-методическое пособие/ Зиангирова Л.Ф.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2015.— 150 c.— Режим доступа: http://www.iprbookshop.ru/31942.— ЭБС «IPRbooks», по паролю

3. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 c.— Режим доступа: http://www.iprbookshop.ru/22425.— ЭБС «IPRbooks», по паролю

5.1.2. Перечень дополнительной литературы:

1. Современные информационные технологии Электронный ресурс : учебное пособие / С.С. Мытько / Д.А. Репечко / И.А. Королькова / А.Р. Ванютин / А.П. Алексеев ; ред. А.П. Алексеев. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2016. - 101 с. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограниченно

2. Синицын Ю.И. Компьютерные сети [Электронный ресурс]: методические указания к лабораторным работам/ Синицын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 114 c.— Режим доступа: http://www.iprbookshop.ru/51533.— ЭБС «IPRbooks», по паролю

3. Чекмарев Ю.В. Вычислительные системы, сети и телекоммуникации [Электронный ресурс]/ Чекмарев Ю.В.— Электрон. текстовые данные.— М.: ДМК Пресс, 2013.— 184 c.— Режим доступа: http://www.iprbookshop.ru/5083.— ЭБС «IPRbooks», по паролю Строганов, М. П. Информационные сети и телекоммуникации [Текст] : учеб. пособие / М. П. Строганов, М. А. Щербаков. - М. : Высшая школа, 2013. - 151 с.

5.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические рекомендации по выполнению практических работ по дисциплине «Информационно-коммуникационные технологии».
2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине «Информационно-коммуникационные технологии».

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Информационные справочные системы:

1. http://biblioclub.ru - ЭБС «Университетская библиотека ОНЛАЙН»
2. http://www.iprbookshop.ru - ЭБС IPRbooks
3. http://biblio-online.ru/ - ЭБС «Biblio-online.ru» издательства «Юрайт» ONLINE»
4. http://www.intuit.ru - Интернет-университет технологий

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы

по дисциплине **«Информационно-коммуникационные технологии»**

для направления подготовки

10.03.01 Информационная безопасность

направленность (профиль) Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Пятигорск, 2023

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание докладов;

– подготовка к семинарам, практическим и лабораторным работам, их оформление;

– составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

– выполнение учебно-исследовательских работ, проектная деятельность;

– подготовка практических разработок и рекомендаций по решению проблемной ситуации;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

– компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

– выполнение курсовых работ (проектов) в рамках дисциплин;

– выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

● подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);

● основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);

● заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационно-коммуникационные технологии» направлена на формирование следующих **компетенций:**

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов

ОПК-2. Способен применять информационно-коммуникационные технологи, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИД-1 ОПК-2 Понимает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. ИД-2 ОПК-2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ИД-3 ОПК-2 Обладает навыки: применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	**Знать:** информационно-коммуникационные технологи, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности **Уметь:** применять и реализовывать информационно-коммуникационные технологи, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности **Владеть:** информационно-коммуникационными технологи, программными средствами системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности
		Знать: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности **Уметь:** понимать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности **Владеть:** современными информационными технологиями и программными средствами, в том числе

		отечественного производства при решении задач профессиональной деятельности
		Знать: навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности **Уметь:** применять навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности **Владеть:** навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;

● формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;

● развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

● формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

● развитие исследовательских умений;

● использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоя-тельной работы	Средства и технологии оценки	Объем часов, в том числе (астр.)		
				СРС	Контактная работа с преподавателем	Всего
4 семестр						
ОПК-2(ИД-1.ИД-2.ИД-3)	Самостоятельное изучение литературы и источников	Конспект	Собеседование	17,01	1,89	18,9
ОПК-2(ИД-1.ИД-2.ИД-3)	Подготовка к практическим занятиям	Опрос	Опрос	4,86	0,54	5,4
ОПК-2(ИД-1.ИД-2.ИД-3)	Подготовка к лекционным занятиям	Опрос	Собеседование	2,43	0,27	2,7
Итого за 4 семестр				**24,3**	**2,7**	**27**

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и

уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

● Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

● Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

● Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

● Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

● Приложение (при необходимости).

Требования к оформлению:

● текст с одной стороны листа;
● шрифт Times New Roman;
● кегль шрифта 14;
● межстрочное расстояние 1,5;
● поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
● доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания

доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	Проект представлен полностью и в срок.
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующим	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	из заданных вопросов, связанных с проектом.	и информационным и технологиями		полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на связанные с проектом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не существенные поручения в групповом проекте.	Проект не сдан.

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент

демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. Берлин А.Н. Телекоммуникационные сети и устройства [Электронный ресурс]/ Берлин А.Н.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 395 c.— Режим доступа: http://www.iprbookshop.ru/52197.— ЭБС «IPRbooks», по паролю

2. Зиангирова Л.Ф. Вычислительные системы, сети и телекоммуникации [Электронный ресурс]: учебно-методическое пособие/ Зиангирова Л.Ф.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2015.— 150 c.— Режим доступа: http://www.iprbookshop.ru/31942.— ЭБС «IPRbooks», по паролю

3. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 c.— Режим доступа: http://www.iprbookshop.ru/22425.— ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Современные информационные технологии Электронный ресурс : учебное пособие / С.С. Мытько / Д.А. Репечко / И.А. Королькова / А.Р. Ванютин / А.П. Алексеев ;

ред. А.П. Алексеев. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2016. - 101 с. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограниченно

2. Синицын Ю.И. Компьютерные сети [Электронный ресурс]: методические указания к лабораторным работам/ Синицын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 114 с.— Режим доступа: http://www.iprbookshop.ru/51533.— ЭБС «IPRbooks», по паролю

3. Чекмарев Ю.В. Вычислительные системы, сети и телекоммуникации [Электронный ресурс]/ Чекмарев Ю.В.— Электрон. текстовые данные.— М.: ДМК Пресс, 2013.— 184 с.— Режим доступа: http://www.iprbookshop.ru/5083.— ЭБС «IPRbooks», по паролю Строганов, М. П. Информационные сети и телекоммуникации [Текст] : учеб. пособие / М. П. Строганов, М. А. Щербаков. - М. : Высшая школа, 2013. - 151 с.

Методическая литература:

1. Методические рекомендации по выполнению практических работ по дисциплине «Информационно-коммуникационные технологии».

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине «Информационно-коммуникационные технологии».

Интернет-ресурсы:

1. http://biblioclub.ru - ЭБС «Университетская библиотека ОНЛАЙН»
2. http://www.iprbookshop.ru - ЭБС IPRbooks
3. http://biblio-online.ru/ - ЭБС «Biblio-online.ru» издательства «Юрайт» ONLINE»
4. http://www.intuit.ru - Интернет-университет технологий