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

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.04 Администрирование сетей

Направление подготовки (специальность)
09.04.01 Информатика и вычислительная техника

Профиль образовательной программы
"Автоматизированные системы обработки информации и управления"

Форма обучения очная

СОДЕРЖАНИЕ

1. Тематическое содержание дисциплины ……3
1.1. Теоретические основы информационных и компьютерных сетей ……..3
1.2. Семиуровневая модель открытых систем OSI ……...7
1.3. Стандарты и стеки протоколов передачи данных в компьютерных сетях …11
1.4. Безопасность информационных и компьютерных систем ……..20

1. Тематическое содержание дисциплины

1.1. Тема 1: «Теоретические основы информационных и компьютерных сетей» (26 часов).

Перечень и краткое содержание рассматриваемых вопросов.

1. Лекция. Обзор архитектуры вычислительных сетей.

Основные определения и термины. Преимущества использования сетей. Архитектура сетей. Сетевое оборудование в локальных, муниципальных, глобальных, беспроводных, домашних сетях. Объединение сетей.

Сеть – это совокупность объектов, образуемых устройствами передачи и обработки данных. Международная организация по стандартизации определила вычислительную сеть как последовательную бит-ориентированную передачу информации между связанными друг с другом независимыми устройствами.

Сети обычно находится в частном ведении пользователя и занимают некоторую территорию и по территориальному признаку разделяются на:

- локальные вычислительные сети (ЛВС) или Local Area Network (LAN), расположенные в одном или нескольких близко расположенных зданиях. ЛВС обычно размещаются в рамках какой-либо организации (корпорации, учреждения), поэтому их называют корпоративными.

- распределенные компьютерные сети, глобальные или Wide Area Network (WAN), расположенные в разных зданиях, городах и странах, которые бывают территориальными, смешанными и глобальными. В зависимости от этого глобальные сети бывают четырех основных видов: городские, региональные, национальные и транснациональные. В качестве примеров распределенных сетей очень большого масштаба можно назвать: Internet, EUNET, Relcom, FIDO.

В состав сети в общем случае включается следующие элементы:

- сетевые компьютеры (оснащенные сетевым адаптером);

- каналы связи (кабельные, спутниковые, телефонные, цифровые, волоконно-оптические, радиоканалы и др.);

- различного рода преобразователи сигналов;

- сетевое оборудование.

Различают два понятия сети: коммуникационная сеть и информационная сеть (рис. 1.1).

Коммуникационная сеть предназначена для передачи данных, также она выполняет задачи, связанные с преобразованием данных. Коммуникационные сети различаются по типу используемых физических средств соединения.

1.2. Преимущества использования сетей.

Информационная сеть предназначена для хранения информации и состоит из информационных систем. На базе коммуникационной сети может быть построена группа информационных сетей:

Под информационной системой следует понимать систему, которая является поставщиком или потребителем информации.

Под каналом связи следует понимать путь или средство, по которому передаются сигналы. Средство передачи сигналов называют абонентским, или физическим, каналом.

Каналы связи (data link) создаются по линиям связи при помощи сетевого оборудования и физических средств связи. Физические средства связи построены на основе витых пар, коаксиальных кабелей, оптических каналов или эфира. Между взаимодействующими информационными системами через физические каналы коммуникационной сети и узлы коммутации устанавливаются логические каналы.

Логический канал – это путь для передачи данных от одной системы к другой. Логический канал прокладывается по маршруту в одном или нескольких физических

каналах. Логический канал можно охарактеризовать, как маршрут, проложенный через физические каналы и узлы коммутации.

Информация в сети передается блоками данных по процедурам обмена между объектами. Эти процедуры называют протоколами передачи данных.

Протокол – это совокупность правил, устанавливающих формат и процедуры обмена информацией между двумя или несколькими устройствами.

Топология компьютерных сетей.

Топология – это описание физических соединений в сети, указывающее какие рабочие станции могут связываться между собой. Тип топологии определяет производительность, работоспособность и надежность эксплуатации рабочих станций, а также время обращения к файловому серверу. В зависимости от топологии сети используется тот или иной метод доступа.

Архитектура – это концепция, определяющая взаимосвязь, структуру и функции взаимодействия рабочих станций в сети. Она предусматривает логическую, функциональную и физическую организацию технических и программных средств сети. Архитектура определяет принципы построения и функционирования аппаратного и программного обеспечения элементов сети.

Архитектура сети определяет основные элементы сети, характеризует ее общую логическую организацию, техническое обеспечение, программное обеспечение, описывает методы кодирования. Архитектура также определяет принципы функционирования и интерфейс пользователя.

В данной лекции будет рассмотрено три вида архитектур:

- архитектура терминал – главный компьютер;
- одноранговая архитектура;
- архитектура клиент – сервер.

2. Лекция. Топология компьютерной сети и методы доступа. Сетевое программное обеспечение.

Виды топологий (Общая шина; Кольцо; Звезда). Методы доступа (CSMA/CD; TPMA; TDMA; FDMA). Иерархия протоколов. Разработка уровней. Службы на основе соединений и службы без установления соединений. Службы и протоколы.

Топология (конфигурация) – это способ соединения компьютеров в сеть. Тип топологии определяет стоимость, защищенность, производительность и надежность эксплуатации рабочих станций, для которых имеет значение время обращения к файловому серверу.

Понятие топологии широко используется при создании сетей. Одним из подходов к классификации топологий ЛВС является выделение двух основных классов топологий: широковещательные и последовательные.

В широковещательных топологиях ПК передает сигналы, которые могут быть восприняты остальными ПК. К таким топологиям относятся топологии: общая шина, дерево, звезда.

В последовательных топологиях информация передается только одному ПК. Примерами таких топологий являются: произвольная (произвольное соединение ПК), кольцо, цепочка.

При выборе оптимальной топологии преследуются три основных цели:

- обеспечение альтернативной маршрутизации и максимальной надежности передачи данных;
- выбор оптимального маршрута передачи блоков данных;
- предоставление приемлемого времени ответа и нужной пропускной способности.

При выборе конкретного типа сети важно учитывать ее топологию. Основными сетевыми топологиями являются: шинная (линейная) топология, звездообразная, кольцевая и древовидная.

Существуют пять основных топологий (рисунок 1.1):
- общая шина (Bus);
- кольцо (Ring);
- звезда (Star);
- древовидная (Tree);
- ячеистая (Mesh).

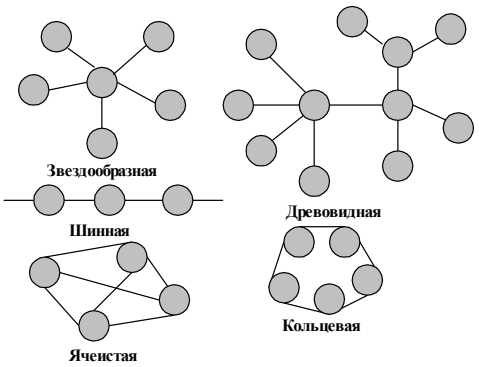

Рисунок 1.1 - Типы топологий

Метод доступа – это способ определения того, какая из рабочих станций сможет следующей использовать ЛВС. То, как сеть управляет доступом к каналу связи (кабелю), существенно влияет на ее характеристики. Примерами методов доступа являются:

- множественный доступ с прослушиванием несущей и разрешением коллизий (Carrier Sense Multiple Access with Collision Detection – CSMA/CD);

- множественный доступ с передачей полномочия (Token Passing Multiple Access – TPMA) или метод с передачей маркера;

- множественный доступ с разделением во времени (Time Division Multiple Access – TDMA);

- множественный доступ с разделением частоты (Frequency Division Multiple Access – FDMA) или множественный доступ с разделением длины волны (Wavelength Division Multiple Access – WDMA).

3. Практическое занятие. Утилита командной строки ipconfig.

Цель работы. Научиться определять сетевые характеристики компьютера при помощи утилиты командной строки ipconfig.

Выполнить задание в соответствии с вариантом.

Номер варианта	Задание
1	Получить подробную информацию о параметрах настройки протокола TCP/IP для всех соединений компьютера (MAC-адрес, IP-адрес, маску подсети, основной шлюз, DHCP и DNS серверы)
2	Обновить аренду IP-адреса на DHCP-сервере для указанного соединения
3	Освободить выделенный IP-адрес для указанного соединения
4	Очистить кэш DNS-клиента
5	Отобразить содержимое кэша DNS-клиента
6	Обновить аренду всех полученных динамических адресов и заново зарегистрировать адреса всех соединений на DNS-сервере
7	Отобразить все идентификаторы DHCP-классов, допустимых для указанного адаптера
8	Установить новый идентификатор класса DHCP для адаптера

4. Практическое занятие. Утилита командной строки ping.

Цель работы. Научиться отправлять эхо-запрос на удаленный хост и получать от него ответ при помощи утилиты ping.

Выполнить задание в соответствии с вариантом

Номер варианта	Задание
1	Послать пакеты на произвольный адрес, завершить операцию вручную
2	Преобразовать IP-адреса в DNS-имена
3	Задать количество посылаемых пакетов
4	Задать размер посылаемого пакета (по умолчанию - 32 байта. Максимальный размер пакета - 65500 байт)
5	Запретить фрагментацию пакетов
6	Задать время жизни пакета (значение от 1 до 255)
7	Задать тип службы (значение от 0 до 255)
8	Отобразить записи маршрута для указанного числа шагов
9	Отобразить штамп времени для указанного числа шагов
10	Задать список хостов, по которому должен быть осуществлен свободный выбор маршрута
11	Задать список хостов, по которому должен быть осуществлен жесткий выбор маршрута
12	Задать время ожидания в миллисекундах при отправке каждого пакета

1.2. Тема 2: «Семиуровневая модель открытых систем OSI» (26 часов).

Перечень и краткое содержание рассматриваемых вопросов.

1. Лекция. Эталонная модель взаимодействия открытых систем.

Общие сведение о модели OSI. Прикладной уровень. Уровень представления данных. Сеансовый уровень. Транспортный уровень. Сетевой уровень. Канальный уровень. Физический уровень.

Для единого представления данных в сетях с неоднородными устройствами и программным обеспечением международная организация по стандартам ISO (International Standardization Organization) разработала базовую модель связи открытых систем OSI (Open System Interconnection). 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. На рис. 2.1 представлена структура базовой модели. Каждый уровень модели OSI выполняет определенную задачу в процессе передачи данных по сети. Базовая модель является основой для разработки сетевых протоколов. OSI разделяет коммуникационные функции в сети на семь уровней, каждый из которых обслуживает различные части процесса области взаимодействия открытых систем.

Рисунок 2.1 - Модель OSI

Модель OSI можно разделить на две различных модели, как показано на рисунке 2.2:

- горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;

- вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.

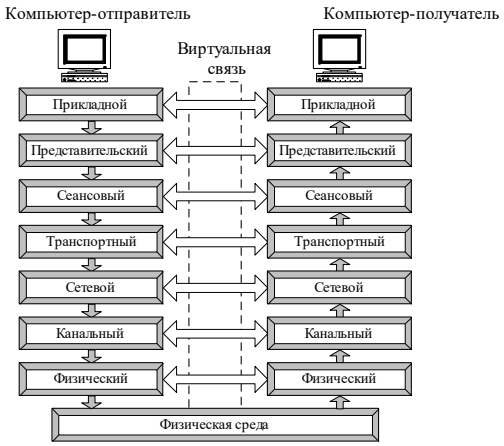

Рисунок **Error! No text of specified style in document.**.2 - Схема взаимодействия компьютеров в базовой эталонной модели OSI

Рассматриваемая модель определяет взаимодействие открытых систем разных производителей в одной сети. Поэтому она выполняет для них координирующие действия по:

- взаимодействию прикладных процессов;
- формам представления данных;
- единообразному хранению данных;
- управлению сетевыми ресурсами;
- безопасности данных и защите информации;
- диагностике программ и технических средств.

На рисунке 2.3 приведено краткое описание функций всех уровней.

7. Прикладной представляет набор интерфейсов, позволяющий получить доступ к сетевым службам
6. Представления преобразует данные в общий формат для передачи по сети
5. Сеансовый поддержка взаимодействия (сеанса) между удаленными процессами
4. Транспортный управляет передачей данных по сети, обеспечивает подтверждение передачи
3. Сетевой маршрутизация, управление потоками данных, адресация сообщений для доставки, преобразование логические сетевые адреса и имена в соответствующие им физические
2. Канальный **2.1. Контроль логической связи (LLC):** формирование кадров **2.2. Контроль доступа к среде (MAC):** управление доступом к среде
1. Физический: битовые протоколы передачи информации

Рисунок **Error! No text of specified style in document.**.1 - Функции уровней

2. Лекция. Оборудование локальных сетей.

Основные типы кабельных сред передачи данных. На сегодня, большая часть компьютерных сетей используют для соединения провода и кабели. Они выступают в качестве среды передачи сигналов между компьютерами. Наиболее распространены: коаксиальный кабель, витая пара, оптоволоконный кабель (таблица 2.1).

Устройства объединения 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. Соотношение между функциями этих устройств и уровнями модели OSI показано на рисунке 2.4.

Существуют следующие классы устройств для объединения сегментов и сетей. Повторитель, который регенерирует сигналы, за счет чего позволяет увеличивать длину сети, работает на физическом уровне. Сетевой адаптер также работает на физическом и отчасти на канальном уровнях.

Таблица 2.1 - Сетевые кабели

Характеристика	Тонкий коаксиальный кабель	Толстый коаксиальный кабель	Витая пара	Оптоволоконный кабель
Эффективная длина кабеля	185 м	500м	100м	2км
Скорость передачи	10 Мбит/с	10 Мбит/с	≥ 10 Мбит/с	≥ 10 Мбит/с
Гибкость	Довольно гибкий	Менее гибкий	Самый гибкий	Не гибкий
Подверженность помехам	Хорошо защищен	Хорошо защищен	Подвержен помехам	Не подвержен помехам

К физическому уровню относится та часть функций сетевого адаптера, которая связана с приемом и передачей сигналов по линии связи, а получение доступа к разделяемой среде передачи, распознавание MAC-адреса компьютера

- это уже функция канального уровня.

Мосты (bridges) и коммутаторы (switches) объединяют сети на канальном уровне и используют функциональные возможности физического уровня. Мосты выполняются на основе компьютера, оснащенного соответствующим ПО. Отличие коммутаторов от мостов в том, что они реализуют свои функции аппаратными средствами и поэтому обладают значительно более высоким быстродействием;

Для мостов сеть представляется набором MAC-адресов устройств. Они извлекают эти адреса из заголовков, добавленных к пакетам на канальном уровне, и используют их во время обработки пакетов для принятия решения о том, на какой порт отправить тот или иной пакет. Мосты не имеют доступа к информации об адресах сетей, относящейся к более высокому уровню. Поэтому они ограничены в принятии решений о возможных путях или маршрутах перемещения пакетов по сети.

Маршрутизаторы работают на сетевом уровне модели OSI. Для маршрутизаторов сеть - это набор сетевых адресов устройств и множество сетевых путей. Маршрутизаторы анализируют все возможные пути между любыми двумя узлами сети и выбирают самый короткий из них.

Шлюз (gateway) - это устройство, выполняющее трансляцию протоколов. Шлюз размещается между взаимодействующими сетями и служит посредником, переводящим сообщения, поступающие из одной сети, в формат другой сети. Шлюз может быть реализован как чисто программными средствами, установленными на обычном компьютере, так и на базе специализированного компьютера.

Фрагмент вычислительной сети (рисунок 2.4) включает основные типы коммуникационного оборудования, для образования локальных сетей и соединения их через глобальные связи друг с другом.

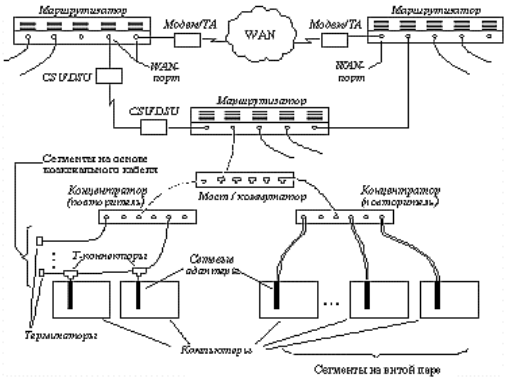

Рисунок 2.4 - Фрагмент сети

Для построения простейшей односегментной сети достаточно иметь сетевые адаптеры и кабель подходящего типа. Но даже в этом простом случае часто используются дополнительные устройства - повторители сигналов, позволяющие преодолеть ограничения на максимальную длину кабельного сегмента.

Основная функция повторителя (repeater), как это следует из его названия - повторение сигналов, поступающих на один из его портов, на всех остальных портах (Ethernet) или на следующем в логическом кольце порте (Token Ring, FDDI) синхронно с сигналами-оригиналами.

Повторитель улучшает электрические характеристики сигналов и их синхронность, и за счет этого появляется возможность увеличивать общую длину кабеля между самыми удаленными в сети станциями.

Многопортовый повторитель часто называют концентратором (hub, concentrator), что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть. Практически во всех современных сетевых стандартах концентратор является необходимым элементом сети, соединяющим отдельные компьютеры в сеть.

3. Практическое занятие. Утилита командной строки tracert.

Цель работы. Научиться определять маршрут до удаленного хоста при помощи утилиты tracert.

Выполнить задание в соответствии с вариантом.

Номер варианта	Задание
1	Отключить разрешение IP-адресов хостов в DNS-имена
2	Задать определенное количество узлов до исследуемого хоста
3	Задать свободный выбор маршрута по указанному списку хостов
4	Задать определенное время ожидания в миллисекундах при отправке каждого пакета
5	Указать имя или IP-адрес хоста, маршрут до которого должен быть исследован

4. Практическое занятие. Утилита командной строки arp.

Цель работы. Научиться просматривать таблицы соответствия IP-адресов MAC-адресам компьютеров и вносить изменений в эту таблицу при помощи утилиты arp.

Выполнить задание в соответствии с вариантом

Номер варианта	Задание
1	Отобразить локальную таблицу соответствия IP-адресов MAC-адресам для всех компьютеров и для конкретного компьютера
2	Вывести на экран данные из таблицы ARP только указанного адаптера
3	Удалить указанный хост из таблицы ARP, удалить сразу несколько адресов из таблицы ARP для всех интерфейсов и для указанного интерфейса
4	Добавить в таблицу ARP статическую запись для всех интерфейсов и для конкретного интерфейса
5	MAC-адрес. Указывается в виде 6 шестнадцатеричных чисел, разделенных дефисами
6	IP-адрес интерфейса. Если адрес интерфейса не указан, то используется первый доступный интерфейс

1.3. Тема 3: «Стандарты и стеки протоколов передачи данных в компьютерных сетях» (32 часа).

Перечень и краткое содержание рассматриваемых вопросов.

1. Лекция. Стек протоколов TCP/IP.

Стек протоколов TCP/IP — набор протоколов передачи данных, используемых в большинстве современных компьютерных сетей. Название TCP/IP происходит из двух протоколов семейства — Transmission Control Protocol (TCP) и Internet Protocol (IP), которые были разработаны и описаны первыми в данном стандарте. В целом же стек протоколов TCP/IP включает в себя четыре уровня: прикладной, транспортный, сетевой и канальный. Протоколы этих уровней полностью реализуют функциональные возможности модели OSI вне зависимости от среды физической передачи.

Протокол IP является одним из самых важных в стеке протоколов TCP/IP. Этот протокол относится к сетевому уровню и объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети, связанными непосредственно или через какое-то количество промежуточных узлов.

Одним из ключевых вопросов построения протокола IP является вопрос сетевой адресации. IP-адрес — это 32-битное число, которое принято записывать при помощи четырех октетов, разделенных точками.

Например:

192.168.0.1

Каждое число (октет) в структуре IP-адреса занимает 1 байт и может лежать в диапазоне от 0 до 255 (с оговоркой, что в последней позиции 0 означает адрес сети, а 255 — широковещательный адрес).

Такой адрес состоит из двух частей — адреса сети и адреса компьютера в данной сети. Такое разделение, как было описано выше, необходимо для маршрутизации пересылаемых пакетов.

Классовая адресация — это исторически первый способ разделения адреса на составные части. Основная идея данного способа заключается в анализе первых нескольких бит адреса для того, чтобы определить «линию разграничения» — первую часть адреса, относящуюся к сети, и вторую часть адреса, относящуюся непосредственно к узлу (табл. 3.1).

Таблица 3.1

Класс	Диапазон значений первого октета	Характеристики адреса
A	0–127	Разделение по первой точке Пример: 10.0.15.1 • адрес сети — 10 • адрес компьютера — 0.15.1
B	128–191	Разделение по второй точке Пример: 172.16.31.2 • адрес сети — 172.16 • адрес компьютера — 31.2
C	192–223	Разделение по третьей точке Пример: 191.168.0.1 • адрес сети — 192.168.0 • адрес компьютера — 1

Как видно из таблицы, сети класса A - это очень большие сети, они могут включать в свой состав до 16 777 216 компьютеров (это число соответствует 224 — именно 24 разряда отдается на адресацию узлов), но таких сетей в мире может быть лишь 128.

Сети класса B имеют меньший размер — до 65 536 компьютеров, при этом таких сетей может быть значительно больше. Еще больше — сетей класса C, эти сети имеют

самый малый размер — до 255 компьютеров.

Адресация на основе сетевой маски (бесклассовая адресация). Основная идея этого способа заключается в том, что дополнительно к IP-адресу компьютеру сообщается и его сетевая маска (32-битное число), на основе которой можно гибко разделить исходный адрес на составные части.

При этом полностью понять смысл разделения адреса на основе маски можно, лишь оперируя адресами в двоичном виде (то есть так, как это делает компьютер). Поясним процедуру разделения на примерах.

Пример:

IP-адрес—192Л68.0.1

Сетевая маска — 255.255.255.0

Маршрутизация.

Итак, разделение адреса требуется для маршрутизации. Маршрутизация - это процесс определения маршрута следования пакетов данных в компьютерной сети.

Маршрутизация предполагает, что каждый компьютер, получивший пакет данных, должен принять решение — передавать этот пакет напрямую либо через промежуточный узел (шлюз). Напрямую пакеты передаются в том случае, когда отправитель и получатель находятся в одной сети. Через шлюз — когда сети разные.

Протокол IPv6.

Протокол IPv6 (Internet Protocol, version 6) — это новая версия протокола IP, призванная решить существующие проблемы традиционной, 4-й версии протокола (иногда называемой IPv4).

Основная из этих проблем — исчерпание пула свободных IP-адресов. В связи с тем, что адрес IPv4 записывается 32-битным числом, общее количество сетевых устройств, имеющих уникальные адреса, не может быть более 232, что составляет примерно 4,3 млрд. Это заметно меньше, чем число потенциальных пользователей Интернета, что является существенным ограничением для развития глобальных коммуникационных систем. К 2015 году пул свободных IP-адресов уже практически исчерпан, дальнейшее уверенное развитие Интернета может быть связано только с внедрением протокола IPv6.

За счет увеличения длины сетевого адреса с 32 до 128 бит адресное пространство IPv6 становится по сути неисчерпаемым. Новый протокол имеет и другие особенности, обеспечивающие преимущества для построения высокопроизводительных компьютерных сетей. Ниже рассмотрим особенности

2. Управление сетями TCP/IP.

Каждый узел в сетях TCP/IP имеет особые настройки, назначаемые в соответствии с требованиями сети. Эти настройки в самом простом случае включают в себя указание адреса, маски, шлюза по умолчанию и сервера DNS, а в более сложных — еще и правил маршрутизации, ограничения трафика, преобразования адресов и др. В данном разделе описываются технологии динамической настройки узлов, организации доступа и защиты в компьютерной сети. Понимание этого материала требуется для планирования сети, а также настройки различных сетевых сервисов, позволяющих реализовать на практике указанные технологии.

Динамическая настройка узлов при помощи DHCP.

Как было показано ранее, для полноценной работы в сети TCP/IP на каждой рабочей станции требуется указать IP-адрес, маску, шлюз по умолчанию и адрес как минимум одного сервера DNS. Все перечисленные параметры могут задаваться вручную, однако более удобным оказывается вариант автоматической настройки параметров сети. Для автоматизации этого процесса, как правило, используется служба DHCP (Dynamic Host Configuration Protocol - протокол динамической настройки узла).

Техническая реализация службы DHCP предполагает, что в сети есть как минимум

один DHCP-сервер, который управляет процессом назначения сетевых параметров рабочим станциям в компьютерной сети. Взаимодействие рабочих станций и сервера осуществляется согласно логике 4 этапов.

1. Обнаружение сервера. На этом этапе рабочая станция, желая получить параметры сети, отправляет широковещательный запрос с целью обнаружить доступные DHCP-серверы. Как правило, такой запрос отправляется в процессе включения рабочей станции — загрузки операционной системы.

2. Предложение. Сервер, получив запрос, подбирает конфигурацию для рабочей станции и отправляет свое предложение, используя аппаратный адрес компьютера, с которого пришел запрос. Заметим, что на этом этапе свои предложения подготовят несколько DHCP-серверов, если они существуют в компьютерной сети.

3. Запрос. Рабочая станция, получив разные предложения от DHCP-серверов, выбирает наиболее подходящее из них и отправляет запрос на выбранную конфигурацию соответствующему серверу.

4. Подтверждение. DHCP-сервер, получив запрос на использование конфигурации, отправляет подтверждение рабочей станции, фиксируя в своей базе данных, что конфигурация закреплена. Рабочая станция, получив подтверждение, настраивает свой сетевой интерфейс согласно выбранной конфигурации.

Межсетевой экран.

Межсетевой экран — это аппаратное устройство или программное средство, которое осуществляет контроль и фильтрацию проходящих сетевых пакетов в соответствии с заданными правилами. Межсетевой экран также часть называют файрволом (от англ, firewall) или брандмауэром (от нем. brandmauer). Все эти термины равнозначны.

В локальный сетях, как правило, межсетевой экран настраивается на маршрутизаторе, обеспечивающем общий доступ локальной сети к Интернету. В этом случае межсетевым экраном контролируется процесс пересылки пакетов данных между внешним и внутренним интерфейсами маршрутизатора, что обеспечивает необходимый уровень доступа и защиту от внешних атак для всей локальной сети.

Межсетевым экраном обычно анализируются следующие параметры пересылаемых пакетов:

1) адрес отправителя или получателя;
2) порт отправителя или получателя;
3) используемый протокол.

На основе анализа указанных параметров межсетевым экраном принимается решение о пересылке или блокировке пакетов. Это позволяет открыть или заблокировать доступ к каким-либо серверам Интернета (или рабочим станциям локальной сети), блокировать возможность использования тех или иных протоколов.

Настройка межсетевого экрана может производиться по белым или черным спискам. В первом случае по умолчанию блокируются все ресурсы, а потом составляется список тех, к которым все же надо предоставить доступ. Во втором случае наоборот, доступ по умолчанию открыт ко всем ресурсам и ведется отдельный список тех из них, к которым доступ надо блокировать. Если используемый вами межсетевой экран позволяет использовать обе стратегии настройки, то выбирайте ту из них, которая позволит лучше контролировать необходимый уровень доступа в соответствии с задачами и кругом пользователей вашей сети.

Отметим, что, помимо простых проверок (адреса, порты, протоколы), доступных во всех реализациях межсетевых экранов, в более «продвинутых» случаях может производиться и дополнительный анализ трафика, связанный с логикой работы сетевых протоколов, количеством запросов, анализом пересылаемых данных и др. Такой анализ позволяет бороться с различными атаками из Интернета, которым могут подвергаться ваши серверы и локальная сеть.

Еще одна задача, которая часто возлагается на межсетевой экран, — это перенаправление портов (пробрасывание портов, port mapping). Перенаправление портов — это технология, которая позволяет получить доступ к ресурсам какого-то компьютера, обращаясь к ним по адресу другого компьютера (маршрутизатора), где настроено перенаправление портов.

В частности, пакеты данных, отправляемые из Интернета на адрес и определенный порт маршрутизатора, могут без изменений пересылаться во внутреннюю сеть - на определенный адрес и порт компьютера, даже если этот компьютер получает доступ к Интернету через NAT. Подобная пересылка пакетов позволяет создавать общедоступные сервисы Интернета на компьютерах, расположенных «внутри» локальной сети. Адресом такого сервиса для пользователей Интернета будет адрес маршрутизатора.

Удаленные подключения VPN.

VPN (Virtual Private Network, виртуальная частная сеть) — обобщенное название технологий, позволяющих создавать сетевые соединения поверх другой сети. В зависимости от решаемых задач и применяемых протоколов, VPN позволяет создавать соединения вида «точка — точка», «точка — сеть», «сеть — сеть».

Не останавливаясь подробно на теоретических основах и особенностях технической реализации VPN, скажем, что данная технология позволяет решить, например, следующие задачи.

1. Предоставить доступ к Интернету клиентам некоторого поставщика услуг. Как правило, подключение к Интернету предусматривает парольный доступ к предоставляемым услугам, учет использованного трафика, защиту передаваемых данных через общедоступные сети. Технологии VPN дают обеспечить выполнение этих условий, предоставить удобный и безопасный доступ к Интернету большому числу пользователей через единый физический канал.

2. Настроить подключение компьютера к удаленной локальной сети. Например, если у вас есть локальная сеть на работе (с выходом в Интернет), то, используя VPN, вы сможете настроить доступ к этой сети с вашего домашнего компьютера (также подключенного к Интернету). Этот доступ будет организован через виртуальный канал, работающий «поверх» Интернета. Виртуальный интерфейс, создаваемый при подключении к удаленной сети, логически не будет отличаться от физических интересов на компьютерах той сети, к которой вы подключаетесь. Ваш домашний компьютер будет иметь полноценный доступ ко всем ресурсам локальной сети, как и компьютеры, имеющие к ней физическое подключение.

3. Соединить территориально удаленные локальные сети в одну локальную сеть. Например, если у некоторой организации есть территориально удаленные офисы, в каждом из которых есть локальная сеть с выходом в городскую сеть или Интернет, то, используя VPN, можно логически объединить эти сети — сделать так, чтобы доступ к компьютерам одного офиса с компьютеров другого офиса логически ничем не отличался от «обычного» доступа в рамках одного физического сегмента локальной сети. Независимо от того, в каком месте расположены ресурсы такой сети, работа с ними будет производиться единообразно независимо от того, из какого офиса соответствующие ресурсы запрашиваются.

Утилиты стека протоколов TCP/IP.

В данном разделе приводится краткое описание некоторых утилит командной строки, предназначенных для получения информации, проверки работоспособности и настройки компьютерных сетей.

Ipconfig.

Утилита Windows для просмотра и обновления информации о сетевых подключениях. В кратком формате (ipconfig) выводит информацию об адресе, маске и основном шлюзе компьютера. В полном формате (ipconfig/all) отображаются подробные сведения обо всех сетевых подключениях.

ifconfig

Команда UNIX и UNIX-подобных операционных систем (Linux, FreeBSD и др.) для просмотра конфигурации и настройки сетевых интерфейсов. Можно сказать, что это аналог утилиты ipconfig, за тем существенным исключением, что утилита ifconfig позволяет не только просматривать, но и настраивать параметры сетевых подключений.

ping

Утилита для проверки соединений в сетях TCP/IP. Принцип работы заключается в том, что утилита отправляет на указанный узел несколько небольших тестовых пакетов и выводит информацию о том, в какой срок были получены ответы.

tracert (traceroute)

Утилита tracert (traceroute — для UNIX-систем) предназначена для определения маршрутов следования данных в сетях TCP/IP. В отличие от утилиты ping, в данном случае отображается не только факт доступности запрашиваемого узла, но и информация по всем узлам маршрута следования пакета.

route

Утилита route позволяет просматривать, удалять и добавлять статические маршруты в таблицу маршрутизации. В Windows просмотр маршрутов осуществляется при помощи вызова этой утилиты с ключом print, добавление и удаление - с ключами add и delete.

nslookup

Утилита, позволяющая в режиме командной строки отправлять обращения к серверам DNS и получать от них самую разнообразную информацию. Эта информация может быть получена как с серверов DNS, указанных по умолчанию, так и с тех серверов, которые указывает сам пользователь.

3. Сетевые службы Интернета.

Поскольку современные локальные сети строятся на основе стека протоколов TCP/IP, то в локальных сетях существует возможность создания сетевых служб, ранее реализованных для Интернета. К таким службам, востребованным в локальных сетях, следует отнести DNS, электронную почту, веб и др. В данном разделе рассматриваются указанные и некоторые другие службы. Освоение предлагаемого материала позволит вам создавать локальные сети, в которых будут представлены собственные сервисы и ресурсы сети Интернет.

Служба DNS.

Как уже было сказано выше, в сетях TCP/IP наряду с числовой адресацией используется и символьный способ именования узлов. С каждым символьным (доменным) именем связывается IP-адрес (или несколько адресов), а с каждым IP-адресом, в свою очередь, может быть связано доменное имя (или несколько доменных имен).

Как хранится информация о соответствии имен и адресов? Каким образом узлы компьютерной сети могут получать эту информацию?

Первый способ реализации системы доменных имен был основан на использовании файлов hosts — текстовых файлов, где хранятся пары соответствий адресов и имен. Предполагалось, что такие файлы должны храниться и регулярно обновляться на всех узлах компьютерной сети.

Очевидно, что этот способ сейчас является устаревшим, так как в современных условиях уже невозможно на каждом компьютере хранить и регулярно обновлять всю информацию обо всех других компьютерах Интернета. Вместе с тем файлы hosts до сих пор используются в большинстве операционных систем — для уточнения информации, хранящейся на серверах DNS. Например, в таких файлах определяется имя сетевой петли — localhost.

Второй способ реализации системы доменных имен основан на использовании службы DNS, представляющей собой распределенную систему, в которой информация о

доменах хранится на большом количестве связанных между собой DNS-серверов.

Домены, зоны и серверы DNS.

DNS - это служба доменных имен, она предполагает, что все компьютеры в сети разделяются на логические группы — домены. При этом доменные имена образуют иерархическую структуру, так как одни домены могут являться частью других. В этой связи выделяют домены первого уровня, второго и т. д.

Зона DNS это часть пространства имен DNS, размещаемая как единое целое на определенном сервере. Каждая зона представляет собой дерево, которое является дочерним по отношению к той зоне, частью которой она является.

Выделение зон является основным механизмом для передачи ответственности (делегирования полномочий) за соответствующую часть домена другому лицу или организации. Именно этот механизм позволяет разделить все пространство доменных имен на части, обслуживаемые разными DNS-серверами.

Таким образом, каждый DNS-сервер хранит только часть информации DNS - информацию о своих зонах. Перечень поддерживаемых зон на каждом конкретном DNS-сервере определяется соответствующими записями на DNS-серверах родительских зон (подробнее об этом будет сказано ниже). Администратор настраивает сервер в соответствии с его ролью в общей системе DNS (включает поддержку соответствующих зон, добавляет в файлы зон необходимую информацию).

Электронная почта.

Служба электронной почты относится к одной из старейших служб Интернета. Данная служба позволяет обмениваться текстовыми сообщениями между компьютерами, подключенными к единой сети. Важно, что такой обмен производится в асинхронном режиме — отправитель и получатель сообщения не обязаны находиться за своими компьютерами одновременно.

Традиционный подход к работе с электронной почтой предполагает использование специальных почтовых клиентов — таких программ, как Outlook Express, The Bat!, Mozilla Thunderbird и др. Почтовый клиент {почтовая программа, клиент электронной почты) — это программное обеспечение, устанавливаемое на компьютере пользователя и предназначенное для получения, хранения, подготовки и отправки сообщений электронной почты одного или нескольких пользователей. Почтовые программы позволяют успешно пользоваться электронной почтой в условиях низкоскоростных и нестабильных каналов связи, в отсутствие постоянного подключения к Интернету.

Создание и настройка сервера электронной почты.

Создание сервера электронной почты возможно на компьютере, имеющем публичный IP-адрес и постоянное подключение к Интернету. Как правило, для этого используется компьютер под управлением Linux или FreeBSD. Настройка почтового сервера возможна и на Windows, однако это чаще всего реализуется в рамках создания более крупных корпоративных систем обмена сообщениями и совместной работы (например, на основе Microsoft Exchange Server).

Для создания полноценного почтового сервера необходимо настроить следующие компоненты.

1. Агент передачи почты {сервер SMTP). Этот агент позволит организовать отправку электронной корреспонденции пользователями вашего почтового сервера другим пользователям Интернета, а также прием и хранение электронных писем на адреса ваших пользователей.

В системах Linux и FreeBSD, как правило, такой агент установлен изначально (обычно используется Sendmail), однако он настроен для приема и пересылки электронной корреспонденции лишь в пределах самого компьютера.

2. Сервер POP3 и IMAP. Данный компонент позволит пользователям вашего почтового сервера «забирать» свою электронную корреспонденцию с почтового сервера по одноименным протоколам.

Для создания сервера POP3 и IMAP необходима установка и настройка соответствующего программного обеспечения, для чего могут использоваться такие пакеты, как Courier Mail Server, Cyrus IMAP server, Dovecot или др.

В наиболее простом варианте такой сервер может использовать системы хранения электронной почты и учетных записей пользователей, принятых в операционной системе (в Linux и FreeBSD — в виде простых текстовых файлов). В сложных конфигурациях могут создаваться собственные базы данных, системы виртуальных почтовых аккаунтов и др. Помимо этого, несмотря на обязательную авторизацию пользователей при получении писем как по протоколу POP3, так и IMAP, дополнительно могут использоваться и криптографические протоколы SSL и TLS, что будет обеспечивать безопасную передачу данных авторизации (логина и пароля), а также шифрование пересылаемых писем.

3. Записи почтовой службы в системе DNS. Эти записи необходимы для того, чтобы внешние почтовые агенты могли «находить» почтовый сервер вашего домена. Например, если вы создаете почтовый сервер для домена vspu.ru (т.е. используете адреса вида name@vspu.ru), то в описании зоны vspu.ru в системе DNS должны быть указаны.

Служба веб.

Интернет как глобальная компьютерная сеть является основой реализации множества сервисов (сетевых служб), обеспечивающих общение пользователей и доступ к информации. Однако среди всех служб Интернета в настоящее время наиболее значимое место занимает служба веб (Web, WWW, Всемирная паутина) — глобальное информационное пространство, основанное на физической инфраструктуре Интернета и протоколе передачи данных HTTP.

Всемирную паутину образуют миллионы веб-серверов Интернета, расположенных по всему миру и обеспечивающих доступ к веб-страницам и другим ресурсам глобальной сети. Информация веб-страниц представлена в виде гипертекста, а для ее просмотра на компьютерах и мобильных устройствах пользователей применяются программы специального назначения — веб-браузеры. Основная функция веб-браузеров — отображение гипертекста, а также сетевая навигация на основе механизма перекрестных ссылок.

В рамках Всемирной паутины возможно, как размещение статической информации, так и создание динамических сайтов, реализация различных сетевых сервисов, среди которых широкую известность получили форумы, чаты, веб-системы электронной почты, а в настоящее время - и большое количество социальных сервисов веб 2.0, позволяющих интернет-пользователям размещать собственную информацию и выстраивать сеть личных отношений в виртуальной среде.

Появление Всемирной паутины кардинальным образом изменило облик Интернета как технической системы, позволило реализовать глобальный информационный ресурс, который в настоящее время ставится в один ряд с системами телевидения и радиовещания, а также с печатными средствами массовой информации.

Протокол HTTP.

HTTP (HyperText Transfer Protocol протокол передачи гипертекста) — протокол передачи данных прикладного уровня, используемый для получения информации с серверов веб. Изначально протокол был предназначен для передачи лишь HTML-документов, а в настоящее время — произвольных данных, включая потоковую передачу видео и звука.

Протокол соответствует клиент-серверной архитектуре, взаимодействие клиента и веб-сервера осуществляется по стандартной схеме «запрос — ответ». При этом каждое HTTP-сообщение (независимо от того, следует оно от клиента к серверу или наоборот) состоит из трех частей: обязательной стартовой строки, заголовка и тела сообщения, Стартовая строка определяет тип сообщения. Если сообщение следует от клиента к серверу (HTTP-запрос), в стартовой строке указывается метод (название операции, которая должна быть выполнена), адрес запрашиваемого ресурса и версия протокола

HTTP. Стартовая строка в сообщении, являющимся ответом сервера (HTTP-ответ), содержит версию протокола, код состояния и текстовое пояснение.

4. Практическое занятие. Утилита командной строки route.

Цель работы. Научиться работать с локальной таблицей маршрутизации при помощи утилиты route.

Выполнить задание в соответствии с вариантом.

Номер варианта	Задание
1	Выполнить очистку таблицы маршрутизации
2	Создать постоянную запись в таблице маршрутов, которая сохраняется после перезагрузки компьютера
3	Вывести на экран локальную таблицу маршрутов, добавить маршрут в таблицу, удалить маршрут из таблицы, изменить имеющийся маршрут.
5	Указать при добавлении маршрута определенную маску подсети
6	Указать при добавлении маршрута адрес шлюза
7	Указать при добавлении маршрута метрику
8	Указать при добавлении маршрута идентификатор интерфейса

5. Практическое занятие. Утилита командной строки pathping.

Цель работы. Научиться получать информацию о задержках в сети и потерях данных при помощи утилиты pathping.

Выполнить задание в соответствии с вариантом.

Номер варианта	Задание
1	Указать свободный выбор маршрута по списку узлов
2	Задать максимальное число прыжков при поиске узла
3	Выполнить трассировку маршрута используя указанный адрес источника
4	Выполнить трассировку маршрута, не определяя имена узлов по адресам
5	Задать произвольную паузу между отправками пакетов (мсек)
6	Выполнить трассировку маршрута, указав число запросов при каждом прыжке
7	Выполнить трассировку маршрута, указав время ожидания каждого ответа (мсек)
8	Указать обязательное использование протокола IPv4
9	Указать обязательное использование протокола IPv6

1.4. Тема 4: «Безопасность информационных и компьютерных систем» (22 часа).

Перечень и краткое содержание рассматриваемых вопросов.

1. Лекция. Основные понятия о защите информации. Основы криптографии. Основные алгоритмы шифрования. Защита соединений. Цифровые подписи. Конфиденциальность электронной переписки. Защита информации в Интернете.

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных. Поэтому обеспечение информационной безопасности является одним из ведущих направлений развития информационных технологий.

Рассмотрим основные понятия защиты информации и информационной безопасности:

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты – сама информация, носитель информации или информационный процесс, в отношении которых необходимо осуществлять защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации – желаемый результат защиты информации. Целью защиты информации может являться предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной потери (утечки) информации или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации – степень соответствия результатов защиты информации по отношению к поставленной цели.

Защита информации от утечки – деятельность по предотвращению распространения защищаемой информации (её разглашения), несанкционированного доступа к защищаемой информации и получения защищаемой информации злоумышленниками.

Защита информации от разглашения – предотвращение несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от несанкционированного доступа – предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами, собственником либо владельцем информации правил доступа к защищаемой информации. Заинтересованным субъектом может быть юридическое лицо, группа физических лиц, общественная организация, отдельное физическое лицо и даже государство.

Система защиты информации – совокупность органов и исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по установленным правилам, которые соответствуют правовым, организационно-распорядительным и нормативным документам по защите информации.

Под информационной безопасностью понимают защищённость информации от незаконного ознакомления, преобразования и уничтожения, а также защищённость информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной. (попытки проникновения злоумышленников, ошибки персонала, выход из строя аппаратных и программных средств, стихийные бедствия (ураган, землетрясение, пожар) и т. п.)

Классификация и содержание возможных угроз информации.

Угрозы безопасности информации в современных системах её обработки

определяются умышленными (преднамеренные угрозы) и естественными (непреднамеренные угрозы), разрушающими и искажающими воздействия внешней среды, надёжностью функционирования средств обработки информации, а также преднамеренных корыстным воздействием несанкционированных пользователей, целями которых являются хищение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации. При этом под умышленными, или преднамеренными, понимаются такие угрозы, которые обусловливаются злоумышленными действиями людей.

Случайными, или естественными, являются угрозы, не зависящие от воли людей. В настоящее время принята следующая классификация угроз сохранности (целостности) информации.

Источники угроз. Под источником угроз понимается непосредственный исполнитель угрозы с точки зрения её негативного воздействия на информацию. Источники можно разделить на следующие группы:

— люди;

— технические устройства;

— модели, алгоритмы, программы;

— технологические схемы обработки;

— внешняя среда.

Предпосылки появления угроз. Существуют следующие предпосылки, или причины появления угроз:

— объективные (количественная или качественная недостаточность элементов системы) – не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

— субъективные – непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.1

Угрозы информационным ресурсам проявляются в овладении конфиденциальной информацией, её модификации в интересах злоумышленника или её разрушении с целью нанесения материального ущерба.

Осуществление угроз информационной безопасности может быть произведено:

- через агентурные источники в органах коммерческих структур, государственного управления, имеющих возможность получения конфиденциальной информации;

- путём подкупа лиц, работающих на предприятии или в структурах, непосредственно связанных с его деятельностью;

- путём перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники, с помощью технических средств разведки и программно-математических воздействий на неё в процессе обработки и хранения;

- путём подслушивания переговоров, ведущихся в служебных помещениях, автотранспорте, в квартирах и на дачах;

- через переговорные процессы с зарубежными или отечественными фирмами, используя неосторожное обращение с информацией.

- через «инициативников» из числа сотрудников, которые хотят улучшить своё благосостояние с помощью «заработка» денег или проявляют инициативу по другим материальным или моральным причинам.

Конфиденциальность электронной переписки.

С развитием коммуникационных средств появилась возможность создания «виртуальных офисов», работу которых невозможно представить без электронной почты. В настоящей статье рассказывается о механизмах некоторых атак, реализуемых злоумышленниками для перехвата почты, нарушения работоспособности рабочей станции

получателя и проникновения в его почтовый ящик. Возможность фальсификации адреса отправителя ввиду своей тривиальности здесь не рассматривается.

В типичной ситуации отправитель пытается послать письмо Получателю, Злоумышленник - перехватить сообщение. Выбор Злоумышленником методики перехвата зависит от взаимного расположения жертв и атакующего.

Ниже мы рассмотрим следующие комбинации.

1. Злоумышленник находится в одном сегменте локальной сети Ethernet либо с Отправителем, либо с Получателем, либо с их почтовым сервером.

2. Отправитель и Получатель находятся в одной локальной сети, к которой злоумышленник имеет доступ через Internet.

3. Отправитель, Получатель и Злоумышленник находятся в различных подсетях, подключенных к Internet.

Проанализировав сложившуюся ситуацию, приходится констатировать: конфиденциальность электронной переписки на сегодняшний день не гарантируется. Угроза исходит не только от спецслужб, наподобие СОРМ, но и от обычных подростков, вооруженных одним лишь модемом, простеньким персональным компьютером и базовыми техническими знаниями. Все атаки, описанные выше, не представляют никакого секрета и хорошо известны как специалистам по безопасности, так и злоумышленникам. Отсутствие громких прецедентов, связанных с хищением почты, не дает повода надевать розовые очки.

2. Практическое занятие. Настройка безопасности в беспроводных сетях.

Цель работы - научиться настраивать безопасность при работе беспроводных сетей, используя расширенные параметры безопасности.

Выполнить задание в соответствии с вариантом.

Номер варианта	Задание
1	Установить надежный пароль администратора на маршрутизаторе
2	Заблокировать доступ к роутеру из Глобальной сети
3	Разрешить доступ к роутеру из Глобальной сети
4	Запретить сообщение идентификатора беспроводной сети маршрутизатором
5	Разрешить сообщение идентификатора беспроводной сети маршрутизатором
6	Обновить прошивку на маршрутизаторе

2. Методические рекомендации по выполнению курсовой работы (проекта) учебным планом не предусмотрено

3. Методические рекомендации по выполнению индивидуальных домашних заданий (контрольных работ) учебным планом не предусмотрено

3.1 Темы индивидуальных домашних заданий учебным планом не предусмотрено