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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.ДВ.08.02 Электронная оргтехника

Направление подготовки (специальность) *09.03.01 Информатика и вычислительная техника*

Профиль образовательной программы **"***Автоматизированные системы обработки информации и управления***"**

Форма обучения *очная*

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1, 2(4 часа).

Тема: «Оргтехника и другие электронные устройства**»**

1.1.1 Краткое содержание вопросов:

1. Введение в дисциплину.

Периферийными или внешними устройствами называют устройства, размещенные вне системного блока и задействованные на определенном этапе обработки информации. Прежде всего - это устройства фиксации выходных результатов: принтеры, плоттеры, модемы, сканеры и т.д. Понятие "периферийные устройства" довольно условное. К их числу можно отнести, например, накопитель на компакт-дисках, если он выполнен в виде самостоятельного блока и соединен специальным кабелем к внешнему разъему системного блока. И наоборот, модем может быть внутренним, то есть конструктивно выполненным как плата расширения, и тогда нет оснований относить его к периферийным устройствам.

Принтеры

Принтеры предназначены для вывода информации на твердые носители, большей частью на бумагу. Существует большое количество разнообразных моделей принтеров, которые различаются по принципу действия, интерфейсу, производительности и функциональным возможностями. По принципу действия различают: матричные, струйные и лазерные принтеры.

Матричные принтеры

До недавнего времени являлись самыми распространенными устройствами вывода информации, поскольку лазерные были дорогими, а струйные малонадежными. Основным преимуществом является низкая

цена и универсальность, то есть возможность печатать на бумаге любого качества.

Принцип действия

Печать происходит при помощи встроенной в печатающий узел матрицы, состоящей из нескольких иголок. Бумага втягивается в принтер с помощью вала. Между бумагой и печатающим узлом располагается красящая лента. При ударе иголки по ленте, на бумаге появляются точки. Иголки, расположенные в печатающем узле управляются электромагнитом. Сам печатающий узел передвигается по горизонтали и управляется шаговым двигателем. Во время продвижения печатающего узла по строке, на бумаге появляются отпечатки символов, состаящие из точек. В памяти принтера хранятся коды отдельных букв, знаков и т.п.. Эти коды определяют, какие иголки и в какой момент следует активизировать для печати определенного символа.

Матрица может иметь 9, 18 или 24 иголки. Качество печати 9-иголочными принтерами невысокая. Для повышения качества, возможна печать 2-х и 4-х кратным прохождением узла по строке. Для современных матричных принтеров стандартом является матрица с 24 иглами. Иголки расположены в два ряда по 12 в каждом. Качество печати значительно выше. Матричные принтеры разрешают печатать сразу несколько копий документа. Для этого листы перекладывают копировальной калькой. Матричные принтеры не требовательны и могут печатать на поверхности любой бумаги - картоне, рулонной бумаге и т.п..

Характеристики матричных принтеров:

- Скорость печати. Измеряется количеством знаков, печатаемых за секунду. Единица измерения cps (character per second - символов в секунду). Производители указывают максимальную скорость печати

в черновом режиме (однопроходная печать). Однако, при выборе принтера следует учитывать, что для режима повышенного качества, а также при выводе графических изображений, скорость значительно ниже.

- Объем памяти. Матричные принтеры оборудованы внутренней памятью (буфером), которая принимает данные от компьютера. В дешевых моделях объем буфера составляет 4-6 Кбайт. В более дорогих больше 200 Кбайт. Чем больше памяти, тем реже принтер обращается к компьютеру за определенной порцией данных, что позволяет центральному процессору выполнять другие задачи. Печать может происходить в фоновом режиме.

- Разрешающая способность. Измеряется количеством точек, печатаемых на одном дюйме. Единица измерения dpi (dot per inch - точек на дюйм). Этот показатель важен для печати графических изображений.

- Цветная печать. Существует несколько моделей цветных матричных принтеров. Но, качество печати 24-иголчатым принтером с применением разноцветной ленты намного хуже, чем качество печати на струйном принтере.

- Шрифты. В памяти многих принтеров хранится широкий набор шрифтов. Но печать может осуществляться любым шрифтом True Type, разработанных для операционной системы Windows.

Струйные принтеры

Первые струйные принтеры выпустила фирма Hewlett Packard. Принцип действия похож на принцип действия матричных принтеров, но вместо иголок в печатающем узле расположены капиллярные распылители и резервуар с чернилами. В среднем, число распылителей от 16 до 64, но

существуют модели, где количество распылителей для черных чернил до 300, а для цветных до 416. Резервуар с чернилами может располагаться отдельно и через капилляры соединяться с печатающим узлом, а может быть встроенным в печатающий узел и заменяться вместе с ним. Каждая конструкция имеет свои недостатки и преимущества. Встроенный в печатающий узел резервуар представляет собой конструктивно отдельное устройство (картридж), его очень легко заменить. Большинство современных струйных принтеров разрешают использовать картриджи для черно-белой и цветной печати.

Принцип действия

Существует два метода распыления чернила: пьезоэлектрический метод и метод газовых пузырьков. В первом, в распылител пьезоэлектрического узла установлен плоский пьезоэлемент, связанный с диафрагмой. При печати он сжимает и разжимает диафрагму, вызывая распыление чернил через распылитель. При попадании потока аэрозоля на носитель, печатается точка (используется в моделях принтеров фирм Epson, Brother). При методе газовых пузырьков, каждый распылитель оборудован нагревающим элементом. При прохождении сквозь элемент микросекундного импульса тока, чернила нагреваются до температуры кипения, и образуются пузырьки, выдавливающие чернила из распылителя, которые образовывают отпечатки на носителе (используется в моделях принтеров фирм Hewlett Packard, Canon).

Цветная печать выполняется путем смешивания разных цветов в определенных пропорциях. Преимущественно, в струйных принтерах реализуется цветовая модель CMYK (Cyan-Magenta-Yellow). Смешивание цветов не может дать чистый черный цвет и потому в составную модели входит черный цвет (Black). При цветной печати картридж имеет 3 или 4 резервуара с чернилами. Печатающий узел проходит по одному месту

листа несколько раз, нанося нужное количество чернил разного цвета. После смешивания чернил, на листе появляется участок нужного цвета.

Характеристики струйных принтеров:

- Скорость печатания. Печать в режиме нормального качества составляет 3-4 страницы в минуту. Цветная печать немного дольше.
- Качество печатания. Дорогие модели струйных принтеров с большим количеством распылителей обеспечивают высокое качество изображения. Но большое значение имеет качество и толщина бумаги. Чтобы избавиться эффекта растекания чернил, некоторые принтеры применяют подогрев бумаги.
- Разрешающая способность. Для печати графических изображений разрешающая способность составляет от 300 до 720 dpi.
- Выбор носителя. Печать невозможна на рулонной бумаге.

Основным недостатком является засыхание чернил в распылителях. Устранить это можно лишь заменой картриджа. Чтобы не допустить засыхания, принтеры оборудованы устройствами очищения распылителей. По цене и качеству струйные принтеры идеально подходят для домашнего пользования. Заправка чернилами не является дорогой и банки чернил хватает на несколько лет.

Лазерные принтеры

Современные лазерные принтеры позволяют достичь более высокого качества печати. Качество приближено к фотографическому. Основным недостатком лазерных принтеров является высокая цена, но цены имеют тенденцию к снижению.

Принцип действия

У большинства лазерных принтеров используется механизм печати, как в копировальных аппаратах. Основным узлом является подвижный барабан, который наносит изображения на бумагу. Барабан представляет собой металлический цилиндр, покрытый слоем полупроводника. Поверхность барабана статически заряжается разрядом. Луч лазера, направленный на барабан, изменяет электростатический заряд в точке попадания и создает на поверхности барабана электростатическую копию изображения. После этого, на барабан наносится слой красящего порошка (тонера). Частицы тонера притягиваются лишь к электрически заряженным точкам. Лист втягивается с лотка и ему передается электрический заряд. При наложении на барабан, лист притягивает на себя частицы тонера с барабана. Для фиксации тонера, лист снова заряжается и проходит между валами, нагретыми до 180 градусов. По окончании, барабан разряжается, очищается от тонера и снова используется.

При цветной печати изображение формируется смешиванием тонеров разного цвета за 4 прохода листа через механизм. При каждом проходе на бумагу наносится определенное количество тонера одного цвета. Цветной лазерный принтер является сложным электронным устройством с 4 резервуарами для тонера, оперативной памятью, процессором и жестким диском, что соответственно увеличивает его габариты и цену.

Основные характеристики лазерных принтеров:

- Скорость печатания. Определяется скоростью механического протягивания листа и скоростью обработки данных, поступающих с компьютера. Средняя скорость печати 4-16 страниц за минуту.
- Разрешающая способность. В современных лазерных принтерах достигает 2400 dpi. Стандартным считается значение в 300 dpi.

- Память. Работа лазерного принтера связана с огромными вычислениями. Например, при разрешающей способности 300 dpi, на странице формата А4 будет почти 9 млн. точек, и нужно рассчитать координаты каждой из них. Скорость обработки информации зависит от тактовой частоты процессора и объема оперативной памяти принтера. Объем оперативной памяти черно-белого лазерного принтера составляет не меньше 1 Мбайт, в цветных лазерных принтерах значительно больше.
- Бумага. Используется качественная бумага формата А4. Существуют модели для формата А3. В некоторых лазерных принтерах есть возможность использования рулонной бумаги.

Срок и качество работы лазерного принтера зависит от барабана. Ресурс барабана дешевых моделей - 40-60 тысяч страниц.

Подсоединение принтера

После физического подсоединения к компьютеру, принтер нужно программно установить и настроить. В Windows процессом печати руководит не программа, а операционная система. Поэтому настройка выполняется с помощью программы Control Panel, после чего принтер становится доступным для всех программ. Управление принтером осуществляют драйверы. Они поставляются вместе с принтером, но драйверы популярных моделей содержатся в комплекте Windows. При отсутствии "родного" драйвера, можно попробовать подобрать похожий из набора существующих драйверов или найти в Интернете на сайте фирмы-производителя.

Сканеры

Сканер - это устройство, позволяющее вводить в компьютер черно-белое или цветное изображения, считывать графическую и текстовую информацию. Сканер используют в случае, когда возникает потребность ввести в компьютер из имеющегося оригинала текст и/или графическое изображение для его дальнейшей обработки (редактирование и т.д.). Ввод такой информации с помощью стандартных устройств ввода требует много времени. Сканированная информация после обрабатывается с помощью специального программного обеспечения (например, программой FineReader) и сохраняется в виде текстового или графического файла.

Принцип действия

Основным элементом сканера является CCD-матрица (Charge Coupled Device - устройство с зарядовой связью) или PMT (PhotoMultiplier Tube - фотомножитель). Колбы-фотомножители используются лишь в сложных и дорогих барабанных профессиональных сканерах, поэтому далее рассмотрен лишь принцип действия сканеров с CCD-матрицей.

CCD-матрица - это набор диодов, которые реагируют на свет при действии внешнего напряжения. От качества матрицы зависит качество распознавания изображения. Дешевые модели распознают наличие/отсутствие цвета, сложные модели - оттенки серого цвета, еще более сложные - все цвета. Сканируемый объект, освещается ксеноновой лампой или набором светодиодов. Отраженный луч с помощью системы зеркал или линз проектируется на CCD-матрицу. Под действием света и внешнего напряжения, матрица генерирует аналоговый сигнал, который изменяется при перемещении относительно ее листа и интенсивности отображения разных элементарных фрагментов. Сигнал подается на аналогово-цифровой преобразователь, где он оцифровуется

(представляется в виде набора нулей и единиц) и передается в память компьютера. Существует два способа сканирования: перемещение листа относительно неподвижной CCD-матрицы или перемещение светочувствительного элемента при неподвижном листе.

Классификация сканеров

Существует немало моделей сканеров, которые различаются методом сканирования, допустимым размером оригинала и качеством оптической системы. По способу организации перемещения считывающего узла относительно оригинала сканеры делятся на планшетные, барабанные и ручные. В планшетных сканерах оригинал кладут на стекло, под которым двигается оптико-электронное считывающее устройство. В барабанных сканерах оригинал через входную щель втягивается барабаном в транспортный тракт и пропускается мимо неподвижного считывающего устройства. Барабанные сканеры не дают возможности сканировать книги, переплетенные брошюры и т.п.. Ручной сканер необходимо плавно перемещать вручную по поверхности оригинала, что не очень удобно. При систематическом использовании лучше иметь, хоть и более дорогой, настольный планшетный сканер.

Основные технические характеристики сканеров:

Разрешающая способность. Сканер рассматривает любой объект как набор отдельных точек (пикселов). Плотность пикселов (количество на единицу площади) называется разрешающей способностью сканера и измеряется в dpi (dots per inch - точек на дюйм). Пиксели располагаются строками, образовывая изображение. Процесс сканирования происходит по строкам, вся строка сканируется одновременно. Обычная разрешающая способность сканера составляет 200-720 dpi. Большее значение (свыше 1000) отображает интерполяционную разрешающую способность,

достигаемую программным путем с использованием математической обработки параметров расположенных возле точек изображения.

Качество отсканированного материала зависит также от оптической разрешающей способности (определяется количеством светочувствительных диодов CCD-матрицы на дюйм) и механической разрешающей способности (определяется дискретностью движения светочувствительного элемента или системы зеркал относительно листа). Выбор разрешающей способности определяется дальнейшим применением результатов сканирования: для художественных изображений, печатаемых на фотонаборных машинах разрешающая способность должна составлять 1000-1200 dpi, для печати изображения на лазерном или струйном принтере - 300-600 dpi, для просмотра изображения на экране монитора - 72-150 dpi, для распознавания текста - 200-400 dpi.

Глубина представления цветов. При преобразовании оригинала в цифровую форму, сохраняются данные о любом пикселе изображения. Простые сканеры определяют наличие или отсутствие цвета, результирующее изображение будет черно-белым. Для представления пикселов достаточно одного разряда (0 или 1). Для передачи оттенков серого между черным и белым цветом необходимо как минимум 4 разряда (16 оттенков) или 8 разрядов (256 оттенков). Чем больше разрядов, тем качественней передаются цвета. Большинство современных цветных сканеров поддерживает глубину цвета 24 разряда. Соответственно, сканер разрешает распознавать около 16 млн. цветов и можно качественно сканировать фотографии. На рынке сканеров есть модели, которые имеют глубину представления цвета 30 и 34 разряда.

Динамический диапазон. Диапазон оптической плотности, определяет спектр полутонов. Оптическая плотность определяется как отношение падающего света к отраженному и колеблется в диапазоне от 0,0

(абсолютно белое тело) до 4,0 (абсолютно черное тело). Значение диапазона дополняется буквой D и определяет степень его чувствительности. Большинство планшетных сканеров имеют стандартный диапазон 2,4 D, неважно различают близкие оттенки одного цвета, но этого достаточно для непрофессионального пользователя.

Метод сканирования. Качество сканированного цветного изображения зависит от метода накопления сканером данных. Различают два основных метода, которые отличаются количеством проходов CCD-матрицы над оригиналом. Первые сканеры использовали 3-проходное сканирование. При каждом проходе сканировался один из цветов палитры RGB. Современные сканеры используют однопроходную методику, которая разделяет световой луч на составляющие с помощью призмы.

Область сканирования. Максимальный размер сканируемого изображения. Ручные сканеры - до 105 мм, барабанные, планшетные сканеры - от формата A4 до Full Legar (8.5'x14').

Скорость сканирования. Нет стандартной методики, которая определяет производительность сканера. Производители указывают количество миллисекунд сканирования одной строки. Но нужно учитывать также способ подсоединения к компьютеру, драйвер, схему передачи цветов, разрешающую способность. Поэтому скорость сканирования определяется экспериментальным путем.

Модемы

Модем - это устройство, предназначенное для подсоединения компьютера к обычной телефонной линии. Название происходит от сокращения двух слов - Модуляция и Демодуляция.

Компьютер вырабатывает дискретные электрические сигналы (последовательности двоичных нулей и единиц), а по телефонным линиям

информация передается в аналоговой форме (то есть в виде сигнала, уровень которого изменяется непрерывно, а не дискретно). Модемы выполняют цифро-аналоговое и аналого-цифровое преобразования. При передаче данных, модемы накладывают цифровые сигналы компьютера на непрерывную частоту телефонной линии (модулируют ее), а при их приеме демодулируют информацию и передают ее в цифровой форме в компьютер. Модемы передают данные по обычным, то есть комутированным, телефонным каналам со скоростью от 300 до 56 000 бит в секунду, а по арендованным (выделенным) каналам скорость может быть и выше. Кроме того, современные модемы осуществляют сжатие данных перед отправлением, и соответственно, реальная скорость может превышать максимальную скорость модема.

По конструктивному выполнению модемы бывают встроенными (вставляются в системный блок компьютера в один из слотов расширения) и внешними (подключаются через один из коммуникационных портов, имеют отдельный корпус и собственный блок питания). Однако, без соответствующего коммуникационного программного обеспечения, важнейшей составляющей которого является протокол, модемы не могут работать. Наиболее распространенными протоколами модемов являются v.32 bis, v.34, v.42 bis и прочие.

Современные модемы для широкого круга пользователей имеют встроенные возможности отправления и получения факсимильных сообщений. Такие устройства называются факсами-модемами. Также, есть возможность поддержки языковых функций, с помощью звукового адаптера.

На выбор типа модема влияют следующие факторы:

- цена: внешние модемы стоят дороже, поскольку в цену входит стоимость корпуса и источника питания;

- наличие свободных портов/слотов: внешний модем подсоединяется к последовательному порту. Внутренний модем к слоту на материнской плате. Если порты или слоты занятые, нужно выбрать одно из устройств;

удобство пользования: на корпусе внешнего модема имеются индикаторы, отображающие его состояние, а также выключатель источника питания. Для установки внешнего модема не нужно разбирать корпус компьютера.

1. 2 Лекция № 3, 4 (4 часа).

Тема: «Понятие электронного документооборота**»**

1.2.1 Вопросы лекции:

1. Общие принципы передачи информации
2. Кодирование сигналов, виды модуляций, пропускная способность канала
3. Каналы передачи информации

1.2.2 Краткое содержание вопросов:

1. Общие принципы передачи информации.

Обмен информацией производится по каналам передачи информации. Каналы передачи информации могут использовать различные физические принципы. Так, при непосредственном общении людей информация передается с помощью звуковых волн, а при разговоре по телефону - с помощью электрических сигналов, которые распространяются по линиям связи. Компьютеры могут обмениваться информацией с использованием

каналов связи различной физической природы: кабельных, оптоволоконных, радиоканалов и др.

Общая схема передачи информации включает в себя отправителя информации, канал передачи информации и получателя информации (рис. 4.1). Если производится двусторонний обмен информацией, то отправитель и получатель информации могут меняться ролями.

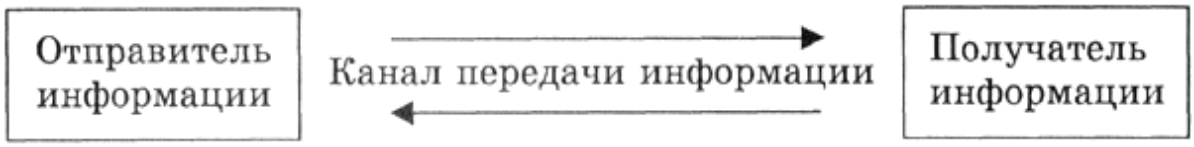


Рис. 4.1. Канал обмена информацией

Основной характеристикой каналов передачи информации является их пропускная способность (скорость передачи информации). Пропускная способность канала равна количеству информации, которое может передаваться по нему в единицу времени.

Обычно пропускная способность измеряется в битах в секунду (бит/с) и кратных единицах Кбит/с и Мбит/с. Однако иногда в качестве единицы измерения используется байт в секунду (байт/с) и кратные ему единицы Кбайт/с и Мбайт/с.

Соотношения между единицами пропускной способности канала передачи информации такие же, как между единицами измерения количества информации:

1 байт/с = 2^3 бит/с = 8 бит/с;

1 Кбит/с = 2^{10} бит/с = 1024 бит/с;

1 Мбит/с = 2^{10} Кбит/с = 1024 Кбит/с;

1 Гбит/с = 2^{10} Мбит/с = 1024 Мбит/с.

2. Кодирование сигналов, виды модуляций, пропускная способность канала.

Передача сообщений по радиоканалу осуществляется путем изменения параметров несущего колебания под воздействием информационного сообщения. При передаче аналоговых сигналов эти параметры изменяются непрерывно и пропорционально их уровню; при передаче цифровых сигналов в зависимости от значений одного или нескольких информационных символов осуществляется манипуляция параметров несущего колебания, то есть они принимают определенные фиксированные значения.

В первой половине XX века разрабатываются и внедряются аналоговые системы радиосвязи и вещания, по которым передаются сигналы телефонии (в том числе многоканальной) и телевидения. В этих системах применяются аналоговые методы модуляции, основанные на изменении параметров гармонической несущей (амплитуды, частоты и фазы) пропорционально величине модулирующего информационного сигнала. Многоканальные системы создаются с использованием частотного разделения каналов. В середине 30-х годов, в связи с развитием импульсной техники, выдвигаются новые идеи создания аналоговых многоканальных систем с импульсными видами модуляции и временным разделением каналов. Аппаратура выделения отдельных каналов в таких системах оказывается более простой по сравнению с системами, в которых используется частотное разделение каналов.

Создаются также системы связи (в основном в диапазоне ВЧ) для передачи сигналов телеграфии. В таких системах осуществляется манипуляция указанных выше параметров гармонического колебания.

В последние двадцать пять лет XX столетия на смену аналоговым методам передачи сообщений приходят и начинают широко внедряться цифровые методы. Цифровые системы связи в начале XXI века полностью заменят аналоговые. Эта революция в области передачи сигналов была подготовлена в 40-х годах, когда были изобретены два исключительно важных для последующего развития техники связи вида преобразования аналоговых сигналов в цифровую форму - импульсно-кодовая и дельта-модуляция.

На совершенствование цифровых методов передачи сигналов значительное влияние оказали положения теории информации, на основе которых во второй половине XX века были созданы помехоустойчивые коды и сложные многопозиционные сигналы. Это позволило обеспечить высокую помехоустойчивость приема сигналов, а также весьма эффективно использовать пропускную способность канала связи.

В середине XX века в связи с проблемами военной радиосвязи рождаются идеи использования в качестве несущего колебания широкополосных сигналов, а не гармонических. Широкое использование таких сигналов в системах фиксированной и подвижной связи начинается в последней четверти XX века.

Рассмотрим более подробно развитие методов передачи аналоговых и цифровых сигналов по радиоканалам.

Аналоговые методы модуляции

В XX веке для передачи сигналов амплитудная (АМ) и частотная (ЧМ) модуляции получили значительное распространение в системах радиосвязи и вещания. Учеными и инженерами всего мира было сделано огромное число исследований и изобретений, направленных на их совершенствование.

Изобретение ЧМ относится к первым годам XX века. Однако в течение почти тридцати лет, до работ знаменитого американского инженера Э. Х. Армстронга, оно не находило практического применения. Начиная с 40-х годов этот вид модуляции получил широчайшее применение в огромном числе систем связи самого различного назначения: подвижной, радиорелейной, спутниковой связи, в ОВЧ-ЧМ вещании. Сотни научных и экспериментальных работ были направлены на исследование искажений ЧМ сигналов, возникающих в линейных цепях связных устройств, и помехоустойчивости приема таких сигналов.

Передачу речи с помощью АМ первым, по-видимому, осуществил один из пионеров радиотехники, американский инженер Фессенден. Модуляция осуществлялась путем включения микрофона, изменяющего затухание в цепи, связывающей передающую антенну и машинный генератор высокой частоты. Этот вид модуляции с 1920 года стал основным в звуковом радиовещании в диапазонах низких, средних и высоких частот (НЧ, СЧ и ВЧ) и сети аналогового АМ вещания, которые уже восемьдесят лет развиваются во всех странах мира. До 40-х годов этот вид модуляции использовался не только в вещании, но также и во всех других видах радиосвязи.

Большое значение для электросвязи имело изобретение американским ученым Карсоном амплитудной модуляции с одной боковой полосой (ОБП), сделанное в 1915 году. Этот метод модуляции позволяет весьма эффективно использовать полосу частот канала связи. Системы с ОБП широко применяются до сих пор в системах многоканальной связи и в телевизионном (ТВ) вещании.

В середине XX века из-за чрезвычайно острой проблемы "тесноты в эфире", сохраняющейся и в настоящее время, были предприняты исследования возможности сокращения полосы канала, необходимой для передачи вещательных сигналов. Модернизация сетей АМ вещания путем их перевода

на ОБП была в середине XX века практически невозможна из-за того, что это требовало замены огромного парка вещательных приемников. Поэтому значительные усилия инженеров были направлены на создание "совместимой ОБП" - нового вида модуляции, с помощью которого можно было бы, с одной стороны, в два раза уменьшить полосу частот, занимаемую каждой станцией, а с другой - сохранить неизменным существующий парк приемников. Такой вид модуляции был предложен в 50-х годах учеными СССР и США. Сокращение занимаемой полосы частот в данном виде модуляции достигалось за счет дополнительной фазовой модуляции АМ сигнала. Несмотря на успешные эксперименты, данный вид модуляции практического применения не нашел. В 80-х годах вновь встал вопрос о сокращении в два раза полосы частот вещательных станций в диапазонах НЧ, СЧ и ВЧ. Этот вопрос исследовался в МСЭ, и его предполагалось решить путем поэтапного внедрения до 2015 года ОБП. Однако к концу XX века стало ясно, что эпоха применения аналоговых методов передачи сигналов по каналам связи завершается, и для этих диапазонов частот были разработаны новые цифровые системы звукового вещания.

В СССР в 1939 году был изобретен еще один метод аналоговой модуляции, названный полярной модуляцией (ПМ). Суть этого метода состоит в том, что положительная полуволна несущей частоты модулируется по амплитуде одним сообщением, а отрицательная - другим. В СССР этот метод был выбран для создания системы стереофонического ОВЧ-ЧМ вещания. Передача стереосигналов осуществлялась путем модуляции методом ПМ поднесущей частоты 31. 25 кГц от двух разнесенных в пространстве микрофонов.

3. Каналы передачи информации.

Для построения компьютерных сетей применяются линии связи, использующие различную физическую среду. В качестве физической среды в

коммуникациях используются: металлы (в основном медь), сверхпрозрачное стекло (кварц) или пластик и эфир. Физическая среда передачи данных может представлять собой кабель "витая пара", коаксиальные кабель, волоконно-оптический кабель и окружающее пространство.

Линии связи или линии передачи данных - это промежуточная аппаратура и физическая среда, по которой передаются информационные сигналы (данные).

В одной линии связи можно образовать несколько каналов связи (виртуальных или логических каналов), например путем частотного или временного разделения каналов. Канал связи - это средство односторонней передачи данных. Если линия связи монопольно используется каналом связи, то в этом случае линию связи называют каналом связи.

Канал передачи данных - это средства двухстороннего обмена данными, которые включают в себя линии связи и аппаратуру передачи (приема) данных. Каналы передачи данных связывают между собой источники информации и приемники информации.

В зависимости от физической среды передачи данных линии связи можно разделить на:

- проводные линии связи без изолирующих и экранирующих оплеток;
- кабельные, где для передачи сигналов используются такие линии связи как кабели "витая пара", коаксиальные кабели или оптоволоконные кабели;
- беспроводные (радиоканалы наземной и спутниковой связи), использующие для передачи сигналов электромагнитные волны, которые распространяются по эфиру.

Проводные линии связи

Проводные (воздушные) линии связи используются для передачи телефонных и телеграфных сигналом, а также для передачи компьютерных данных. Эти линии связи применяются в качестве магистральных линий связи.

По проводным линиям связи могут быть организованы аналоговые и цифровые каналы передачи данных. Скорость передачи по проводным линиям "простой старой телефонной линии" (POST - Primitive Old Telephone System) является очень низкой. Кроме того, к недостаткам этих линий относятся помехозащищенность и возможность простого несанкционированного подключения к сети.

Кабельные линии связи

Кабельные линии связи имеют довольно сложную структуру. Кабель состоит из проводников, заключенных в несколько слоев изоляции. В компьютерных сетях используются три типа кабелей.

Витая пара (twisted pair) — кабель связи, который представляет собой витую пару медных проводов (или несколько пар проводов), заключенных в экранированную оболочку. Пары проводов скручиваются между собой с целью уменьшения наводок. Витая пара является достаточно помехоустойчивой. Существует два типа этого кабеля: неэкранированная витая пара UTP и экранированная витая пара STP.

Характерным для этого кабеля является простота монтажа. Данный кабель является самым дешевым и распространенным видом связи, который нашел широкое применение в самых распространенных локальных сетях с архитектурой Ethernet, построенных по топологии типа “звезда”. Кабель подключается к сетевым устройствам при помощи соединителя RJ45.

Кабель используется для передачи данных на скорости 10 Мбит/с и 100 Мбит/с. Витая пара обычно используется для связи на расстояние не более нескольких сот метров. К недостаткам кабеля "витая пара" можно отнести возможность простого несанкционированного подключения к сети.

Коаксиальный кабель (coaxial cable) - это кабель с центральным медным проводом, который окружен слоем изолирующего материала для того, чтобы отделить центральный проводник от внешнего проводящего экрана (медной оплетки или слой алюминиевой фольги). Внешний проводящий экран кабеля покрывается изоляцией.

Существует два типа коаксиального кабеля: тонкий коаксиальный кабель диаметром 5 мм и толстый коаксиальный кабель диаметром 10 мм. У толстого коаксиального кабеля затухание меньше, чем у тонкого. Стоимость коаксиального кабеля выше стоимости витой пары и выполнение монтажа сети сложнее, чем витой парой.

Коаксиальный кабель применяется, например, в локальных сетях с архитектурой Ethernet, построенных по топологии типа “общая шина”.

Коаксиальный кабель более помехозащищенный, чем витая пара и снижает собственное излучение. Пропускная способность – 50-100 Мбит/с. Допустимая длина линии связи – несколько километров. Несанкционированное подключение к коаксиальному кабелю сложнее, чем к витой паре.

Кабельные оптоволоконные каналы связи. Оптоволоконный кабель (fiber optic) – это оптическое волокно на кремниевой или пластмассовой основе, заключенное в материал с низким коэффициентом преломления света, который закрыт внешней оболочкой.

Оптическое волокно передает сигналы только в одном направлении, поэтому кабель состоит из двух волокон. На передающем конце оптоволоконного кабеля требуется преобразование электрического сигнала в световой, а на приемном конце обратное преобразование.

Основное преимущество этого типа кабеля – чрезвычайно высокий уровень помехозащищенности и отсутствие излучения. Несанкционированное подключение очень сложно. Скорость передачи данных 3Гбит/с. Основные недостатки оптоволоконного кабеля – это сложность его монтажа, небольшая механическая прочность и чувствительность к ионизирующим излучениям.

Беспроводные (радиоканалы наземной и спутниковой связи) каналы передачи данных

Радиоканалы наземной (радиорелейной и сотовой) и спутниковой связи образуются с помощью передатчика и приемника радиоволн и относятся к технологии беспроводной передачи данных.

Радиорелейные каналы передачи данных

Радиорелейные каналы связи состоят из последовательности станций, являющихся ретрансляторами. Связь осуществляется в пределах прямой видимости, дальности между соседними станциями - до 50 км. Цифровые радиорелейные линии связи (ЦРРС) применяются в качестве региональных и местных систем связи и передачи данных, а также для связи между базовыми станциями сотовой связи.

Спутниковые каналы передачи данных

В спутниковых системах используются антенны СВЧ-диапазона частот для приема радиосигналов от наземных станций и ретрансляции этих сигналов обратно на наземные станции. В спутниковых сетях используются три основных типа спутников, которые находятся на геостационарных орбитах, средних или низких орбитах. Спутники запускаются, как правило, группами. Разнесенные друг от друга они могут обеспечить охват почти всей поверхности Земли. Работа спутникового канала передачи данных представлена на рисунке

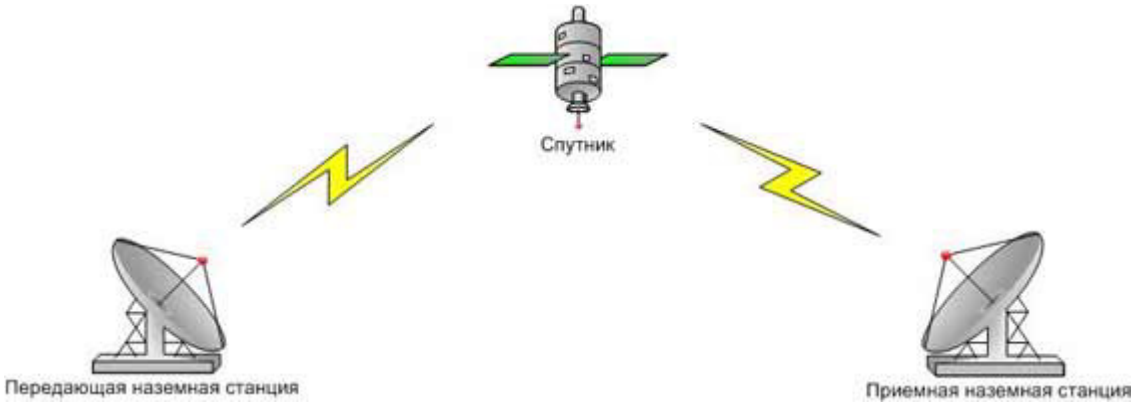


Рис. 1.

Целесообразнее использовать спутниковую связь для организации канала связи между станциями, расположенными на очень больших расстояниях, и возможности обслуживания абонентов в самых труднодоступных точках. Пропускная способность высокая – несколько десятков Мбит/с.

Сотовые каналы передачи данных

Радиоканалы сотовой связи строятся по тем же принципам, что и сотовые телефонные сети. Сотовая связь - это беспроводная телекоммуникационная система, состоящая из сети наземных базовых приемо-передающих станций и сотового коммутатора (или центра коммутации мобильной связи).

Базовые станции подключаются к центру коммутации, который обеспечивает связь, как между базовыми станциями, так и с другими телефонными сетями и с глобальной сетью Интернет. По выполняемым функциям центр коммутации аналогичен обычной АТС проводной связи.

LMDS (Local Multipoint Distribution System) - это стандарт сотовых сетей беспроводной передачи информации для фиксированных абонентов. Система строится по сотовому принципу, одна базовая станция позволяет охватить район радиусом несколько километров (до 10 км) и подключить несколько тысяч абонентов. Сами БС объединяются друг с другом высокоскоростными наземными каналами связи либо радиоканалами. Скорость передачи данных до 45 Мбит/с.

Радиоканалы передачи данных WiMAX (Worldwide Interoperability for Microwave Access) аналогичны Wi-Fi. WiMAX, в отличие от традиционных технологий радиодоступа, работает и на отраженном сигнале, вне прямой видимости базовой станции. Эксперты считают, что мобильные сети WiMAX открывают гораздо более интересные перспективы для пользователей, чем фиксированный WiMAX, предназначенный для корпоративных заказчиков. Информацию можно передавать на расстояния до 50 км со скоростью до 70 Мбит/с.

Радиоканалы передачи данных MMDS (Multichannel Multipoint Distribution System). Эти системы способна обслуживать территорию в радиусе 50—60

км, при этом прямая видимость передатчика оператора является не обязательной. Средняя гарантированная скорость передачи данных составляет 500 Кбит/с — 1 Мбит/с, но можно обеспечить до 56 Мбит/с на один канал.

Радиоканалы передачи данных для локальных сетей. Стандартом беспроводной связи для локальных сетей является технология Wi-Fi. Wi-Fi обеспечивает подключение в двух режимах: точка-точка (для подключения двух ПК) и инфраструктурное соединение (для подключения несколько ПК к одной точке доступа). Скорость обмена данными до 11 Мбит/с при подключении точка-точка и до 54 Мбит/с при инфраструктурном соединении.

Радиоканалы передачи данных Bluetooht - это технология передачи данных на короткие расстояния (не более 10 м) и может быть использована для создания домашних сетей. Скорость передачи данных не превышает 1 Мбит/с.

1.3 Лекция № 5, 6 (4 часа).

Тема: «Устройства создания электронных документов**»**

1.3.1 Вопросы лекции:

1) Компьютер: текстовые и табличные процессоры

2) Объектно-ориентированные среды формирования документов

3) Телеграф, телекс, телетекст

1.3.2 Краткое содержание вопросов:

1 Компьютер: текстовые и табличные процессоры

Табли́чный проце́ссор —категория программного обеспечения, предназначенного для работы сэлектронными таблицами. Изначально табличные редакторы позволяли обр абатывать исключительнодвухмерные таблицы, прежде всего с числовыми да нными, но затем появились продукты, обладавшиепомимо этого возможност ью включать текстовые, графические и другие мультимедийные элементы.Ин струментарий электронных таблиц включает мощные математические функц ии, позволяющие вестисложные статистические, финансовые и прочие расче ты.

Электро́нные табли́цы (или табличные процессоры) - это прикладные программы, предназначенные дляпроведения табличных рас четов. Появление электронных таблиц исторически совпадает с началомрасп ространения персональных компьютеров. Первая программа для работы с эле ктронными таблицами— табличный процессор, была создана в 1979 году, предназначалась для компь ютеров типа Apple II иназывалась VisiCalc. В 1982 году появляется знаменит ый табличный процессор Lotus 1-2-3,предназначенный для IBM PC. Lotus объединял в себе вычислительные воз можности электронных таблиц,деловую графику и функции реляционной СУ БД. Популярность табличных процессоров росла оченьбыстро. Появлялись н овые программные продукты этого класса: Multiplan, Quattro Pro, SuperCalc и другие.Одним из самых популярных табличных процессоров сегодня являет ся MS Excel, входящий в составпакета Microsoft Office.

Что же такое электронная таблица? Это средство информационных тех нологий, позволяющее решатьцелый комплекс задач: Прежде всего, выполне ние вычислений. Издавна многие расчеты выполняются втабличной форме, о собенно в области делопроизводства: многочисленные расчетные ведомости, табуляграммы, сметы расходов и т. п. Кроме того, решение численными мето дами целого рядаматематических задач; удобно выполнять в табличной форм е. Электронные таблицы представляют собойудобный инструмент для автома

тизации таких вычислений. Решения многих вычислительных задач наЭВМ, которые раньше можно было осуществить только путем программирования, стало возможнореализовать Математическое моделирование. Использование математических формул в ЭТ позволяетпредставить взаимосвязь между разл ичными параметрами некоторой реальной системы. Основноесвойство ЭТ — мгновенный пересчет формул при изменении значений входящих в них опер андов.Благодаря этому свойству, таблица представляет собой удобный инстр умент для организации численногоэксперимента:

1. подбор параметров,
2. прогноз поведения моделируемой системы,
3. анализ зависимостей,
4. планирование.

Дополнительные удобства для моделирования дает возможность графи ческого представления данных(диаграммы); Использование электронной таб лицы в качестве базы данных. Конечно, по сравнению с СУБДэлектронные т аблицы имеют меньшие возможности в этой области. Однако некоторые опер ациииманипулирования данными, свойственные реляционным СУБД, в них ре ализованы. Это поиск информациипо заданным условиям и сортировка инфо рмации.

В электронных таблицах предусмотрен также графический режим рабо ты, который дает возможностьграфического представления (в виде графиков, диаграмм) числовой информации, содержащейся втаблице.

Основные типы данных: числа, как в обычном, так и экспоненциальн ом формате, текст –

последовательность символов, состоящая из букв, цифр и пробелов, формулы . Формулы должныначинаться со знака равенства, и могут включать в себя чи сла, имена ячеек, функции (математические,статистические, финансовые, тек стовые, дата и время и т.д.) и знаки математических операций.

Электронные таблицы просты в обращении, быстро осваиваются непро фессиональными пользователямикомпьютера и во много раз упрощают и уск оряют работу бухгалтеров, экономистов, ученых.

Основные элементы электронных таблиц:

1. Столбец,
2. Заголовки столбцов,
3. Строка,
4. Заголовки строк,
5. Неактивная ячейка,
6. Активная ячейка.

История

Идею электронных таблиц впервые сформулировал американский учен ый Ричард Маттессич, опубликовавв 1961 г. исследование под названием «Bu dgeting Models and System Simulation». Концепцию дополнили в1970 г. Пардо и Ландау, подавшие заявку на соответствующий патент (U.S. Patent 4,398,24 9 (англ.)).Патентное ведомство отклонило заявку, но авторы через суд добил ись отмены этого решения.

Общепризнанным родоначальником электронных таблиц как отдельног о класса ПО является Дэн Бриклин,совместно с Бобом Фрэнкстоном разработ авший легендарную программу VisiCalc в 1979 г. Этот табличныйредактор дл я компьютера Apple II стал «убойным приложением», превратившим персона льный компьютериз экзотической игрушки для технофилов в массовый инстр умент для бизнеса.

Впоследствии на рынке появились многочисленные продукты этого кла сса - SuperCalc, Microsoft MultiPlan,Quattro Pro, Lotus 1-2-3, Microsoft Excel, OpenOffice.org Calc, таблицы AppleWorks и gnumeric,мини малистический Spread32.

Существует табличный процессор для мобильных телефонов и КПК по д названием SpreadCE.

2. Объектно-ориентированные среды формирования документов.

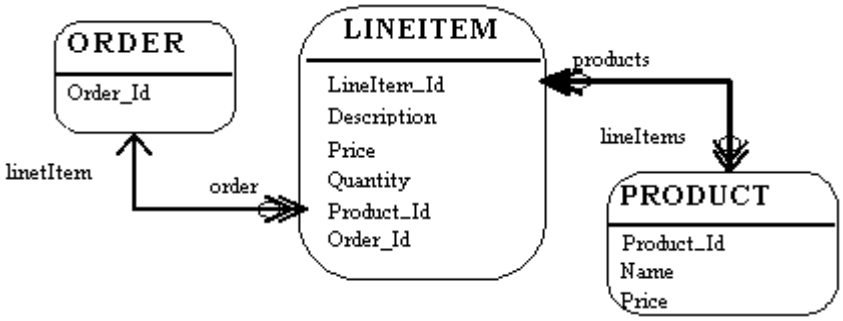
Реляционные базы данных и объектно-ориентированные среды не могут похвастаться полной совместимостью. Они представляют собой два разных видения мира: в реляционных базах данных вы оперируете данными, а в объектно-ориентированных средах - поведением. Нельзя сказать, что одно из этих видений лучше другого: объектно-ориентированные системы обычно лучше подходят для сложных систем со сложным поведением, в которых данные вторичны, а также для систем, в которых данные структурированы иерархически (например, при работе с ведомостями). Реляционные базы данных отлично подходят для создания отчетов и систем, в которых используются динамические и неструктурированные связи между компонентами.

Важное обстоятельство заключается в том, что огромное количество данных хранится в реляционных базах данных, и если объектно-ориентированные системы должны работать с этими данными, они должны уметь обмениваться данными с реляционными СУБД. Кроме того, объектно-ориентированным системам часто приходится обмениваться данными с необъектно-ориентированными системами. В таких ситуациях реляционные СУБД представляют собой естественный механизм обмена данными.

Хотя у объектно-ориентированных и реляционных систем есть общие черты (атрибуты объектов по духу схожи со столбцами записей базы данных), существует ряд фундаментальных различий, значительно осложняющих интеграцию. Одно из фундаментальных различий заключается в том, что реляционные модели экспортируют данные (в виде значений столбцов), а объектные - скрывают данные (инкапсулируют их за общими интерфейсами).

Реляционная модель

В реляционной модели оперируют терминами объектов и взаимосвязей. Объектом может быть физическая таблица или логическая проекция нескольких таблиц, которую могут называть представлением. На следующем рисунке показаны таблицы LINEITEM, ORDER и PRODUCT и взаимосвязи между ними. В реляционной модели присутствуют следующие элементы:



Реляционная модель

У объекта есть столбцы. У каждого столбца есть имя и тип. На рисунке выше у объекта LINEITEM есть столбцы LineItem_Id (основной ключ), Description, Price, Quantity, Product_Id и Order_Id (последние два столбца - внешние ключи, привязывающие объект LINEITEM к объектам ORDER и PRODUCT).

Объект содержит записи (строки). Каждая строка представляет собой уникальный набор данных, обычно представляющий собой набор хранимых характеристик объекта.

У каждого объекта есть один или несколько основных ключей. LineItem_Id - основной ключ объекта LINEITEM.

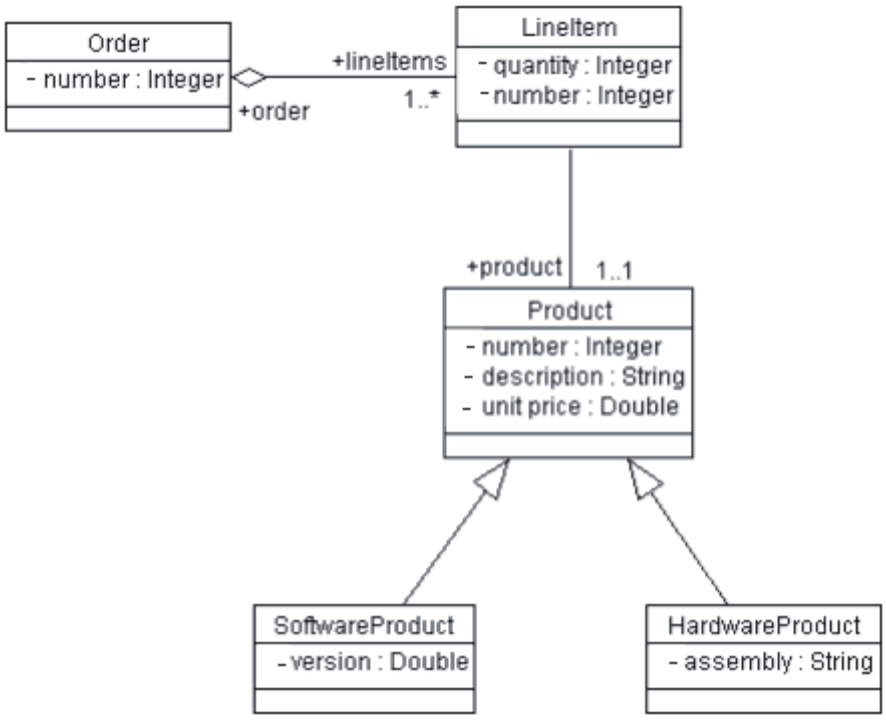
Особенности поддержки взаимосвязей зависят от разработчика базы данных. В данном примере продемонстрирована логическая модель с взаимосвязью между таблицами PRODUCT и LINEITEM. В физической модели взаимосвязи обычно реализованы в виде ссылок между внешними и основными ключами. Если один объект ссылается на другой, в нем будут

столбцы с внешними ключами. В столбцах с внешними ключами хранятся данные, по которым можно установить взаимосвязь между записями данного объекта и записями взаимосвязанного объекта.

У взаимосвязей есть понятие множественности. Типичные примеры множественности - один к одному (1:1), один ко многим (1:m), многие к одному(m:1) и многие ко многим (m:n). В данном примере у LINEITEM взаимосвязь 1:1 с PRODUCT, а у PRODUCT взаимосвязь 0:m с LINEITEM.

Объектная модель

В объектной модели, помимо прочего, присутствуют классы (полное описание объектной модели можно найти в книге [UML01]). Классы задают структуру и поведение набора объектов, которые иногда называют**экземплярами** объектов. Структура задается в виде набора атрибутов (значений данных) и связей (связей между классами). На следующем рисунке показана простая диаграмма класса, на которой отмечены только атрибуты (данные) класса.



Объектная модель (диаграмма класса)

У атрибута Order есть атрибут number (номер заказа) и связь с одним или несколькими атрибутами Line. У каждого атрибута Line есть атрибут quantity (количество заказанных единиц товара).

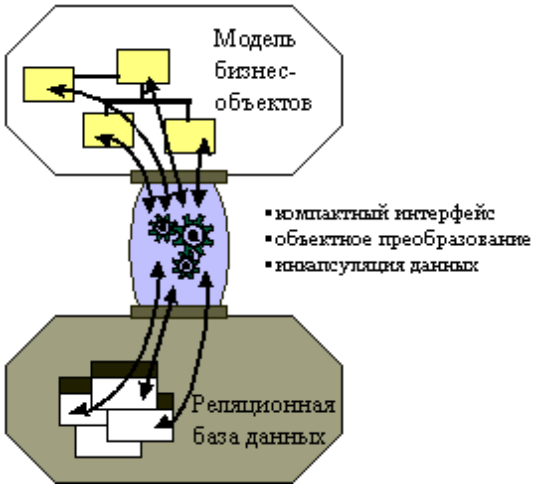
Объектная модель поддерживает наследование. Класс может наследовать данные и поведение у другого класса (например, продукты SoftwareProduct и HardwareProduct могут наследовать атрибуты и методы у класса Product).

Среды хранения

Большинство бизнес-приложений пользуются реляционными системами для физического хранения данных. Сложность для разработчиков объектно-ориентированных приложений заключается в том, чтобы отделить и инкапсулировать реляционную базу данных в достаточной мере для того, чтобы изменения в ней не "сломали" объектную модель и наоборот. Существует множество решений, в которых приложения напрямую обращаются к реляционным базам данных, однако проблема состоит в обеспечении прозрачной интеграции объектной и реляционной моделей.

Существует несколько стандартных интерфейсов (API) для работы с базами данных, например Microsoft Open Data Base Connectivity (ODBC). Все эти интерфейсы закрыты (взаимодействуют с конкретными реализациями СУБД). Интерфейсы API поддерживают язык управления данными (DML), применяемый приложениями для работы с реляционными базами данных. Для применения реляционных данных в объектно-ориентированных приложениях требуется преобразование этих данных в объектно-ориентированный формат. Для преобразования выборки данных в объекты приложения требуется довольно весомый программный код. Цель объектно-реляционной среды заключается в инкапсуляции физического хранилища

данных и предоставлении функции преобразования данных в объектный формат.



Назначение среды хранения

Около 30% времени разработчики приложений тратят на организацию доступа к реляционным базам данных из объектно-ориентированных приложений. Если объектно-ориентированный интерфейс реализован неправильно, это время можно считать потерянным. Создание объектно-реляционной среды позволяет избежать таких потерь. Применение объектно-реляционной среды в приложениях позволяет сократить стоимость организации доступа к реляционным базам данных до менее чем 10% общей стоимости реализации. Важнейший компонент стоимости, который следует принимать во внимание при реализации, - обслуживание. Свыше 60% общей стоимости системы на протяжении ее жизненного цикла составляет обслуживание. Плохо реализованная объектно-реляционная система может стать настоящим кошмаром при обслуживании системы как с технической, так и с финансовой точек зрения.

3.Телеграф, телекс, телетекст

Телеграф - способ передачи кодированной побуквенно информации по проводам. Первоначально специальным кодом (Морзе, Бодо и другими),

затем кодом, унифицированным с ЭВМ и другими средствами хранения информации (МТК-2, КОИ-7 и др.), что позволило посылать при помощи не ключа, а клавиатуры, а принимать не в виде точек и тире на ленте, а в виде напечатанных букв. Ранее употреблялся также неэлектрический (оптический) телеграф.

Буквопечатающий телеграф также в просторечии именуется **телетайп**, хотя, строго говоря, телетайп это лишь одна из марок (копирайт фирмы Teletype) буквопечатающего аппарата, ставшая общим названием (как ксерокс - из фирменной марки Xerox в общее понятие), и более распространены другие модели телеграфных аппаратов (СТК-2, сохранившийся в почтовых отделениях и особенный печатанием не на лист, а на наклеиваемую затем ленту, а также использованием 5-, а не 7-битного кода, Т-63, Т-100 и др.).

Международная сеть абонентского телеграфа, в которой можно связываться, набирая номер, как в обычном телефоне, называется Телекс. В СССР аналогичная система именовалась АТ ("Телексом", впрочем, также пользовались, но в основном предприятия, ведущие внешнеторговую деятельность и организации, ведущие международную). Наряду с АТ использовалась система ПС, реализовывавшая протокол, схожий с IP, но маршрутизировались не пакеты, а сообщения целиком. Интересно отметить, что эта электромеханическая система была внедрена ещё в 1949 году. В настоящее время они вытеснены протоколом передачи телеграмм по IP, и понятие "Телекс" означает прежде всего саму международную телеграмму.

Телефакс - понятие иного логического ряда. Это система передачи изображений, а не буквенных сообщений, используя обычную (телефонную) сеть. Факс класса 1 (фототелеграф) использовал телеграфные линии и, как правило, приём на фотобумагу, в настоящее время практически вымер. Факс класса 3 и 4 (класс 2 не нашёл употребления) использует передачу в полосе телефонной связи с использованием квадратурного кодирования и

специализированный алгоритм сжатия изображений. В настоящее время также вытесняется передачей изображений по IP, с использованием сканеров и принтеров, подсоединённых к обычному компьютеру, но, ввиду распространённости, ещё продолжает употребляться. Существуют протоколы, эмулирующие телефакс на компьютере, используя модемы.

1.4 Лекция № 7 (2 часа).

Тема: «Физические среды и протоколы передачи данных**»**

1.4.1 Вопросы лекции:

1) Модем и его протоколы

2) FAX-протоколы

3) Протоколы локальных сетей физического уровня: Ethernet, ARCnet, Token Ring.

1.4.2 Краткое содержание вопросов:

1. Модем и его протоколы.

Первый модем появился в 1958 году. Американская телефонная компания AT&T ввела дейтафонное обслуживание (передача информации по телефонному каналу). Первым модемом был Bell Dataphone 103, скорость передачи которого составляла 300 бит/с. Но даже сегодня большинство модемов имеет режим работы, совместимый с Bell 103. Bell 212a предложил уже 1200 бит/с, правда был более чувствителен к шумам в телефонной

линии. Менее шумочувствительный модем разработала компания Racal-Vadic. К сожалению, эти две модели модемов несовместимы. Так начиналось длительное соперничество за права и стандарты в мире модемов.

В последнее время модемы становятся неотъемлемой частью компьютера, который превратился в интеллектуальное многофункциональное устройство, предоставляющее пользователю возможность общаться с огромным миром информации со всего света. Благодаря установки модема на компьютер, последний фактически превращается в звено глобальной сети.

Модем позволяет, не выходя из дома, помимо широчайшего спектра информации и услуг, получаемых через Internet, разместить сообщение на BBS (электронной доске объявлений), скопировать с той же BBS интересующие файлы. Кроме того, воспользовавшись глобальными сетями (RelCom, FidoNet) можно принимать и посылать электронные письма не только внутри города, но фактически в любой конец земного шара. Глобальные сети дают возможность не только обмениваться почтой, но и участвовать во всевозможных конференциях, получать новости практически по любой интересующей тематике.

Модем– это устройство для обмена информации с другими компьютерами через сеть (телефонную).

Факс-модем– это устройство сочетающее возможности модема и средства для обмена факсимильными сообщениями с другими факс – модемам и обычными телефонными аппаратами.

Модемы – это устройства предназначенные для передачи информации через телефонную сеть.

Модем – это устройство прямого(модулятор) и обратного(демодулятор) преобразования сигнала принятого для использования в определенном канале связи.

Модем преобразует цифровой сигнал в аналоговый, этот процесс называется модуляцией, обратный процесс – демодуляцией.

IBM-модем-телефонная сеть-модем-IBM

Цифровые данные поступающие в модем из компьютера преобразуются в нем путем модуляции и направляются в телефонную линию. Модем-приемник принимает данные по протоколу осуществляет обратное преобразование и пересылает восстановленные цифровые данные в свой компьютер.

Протоколы MNP -протоколы коррекции ошибок нижнего уровня.

При передаче данных по зашумленным телефонным линиям, как уже говорилось выше, всегда существует вероятность, что данные, передаваемые одним модемом, будут приняты другим модемом в искаженном виде - некоторые передаваемые байты могут изменить свое значение или даже просто исчезнуть.

Для того, чтобы пользователь имел гарантии, что его данные переданы без ошибок, используются протоколы коррекции ошибок.

Общая форма передачи данных по протоколам с коррекцией ошибок следующая: данные передаются отдельными блоками (пакетами) по 16-20000 байт, в зависимости от качества связи. Каждый блок снабжается заголовком, в котором указана проверочная информация, например контрольная сумма блока. Принимающий компьютер самостоятельно подсчитывает контрольную сумму каждого блока и сравнивает ее с контрольной суммой из заголовка блока. Если эти две контрольный суммы совпали, принимающая

программа считает, что блок передан без ошибок. В противном случае принимающий компьютер передает передающему запрос на повторную передачу этого блока.

Протоколы коррекции ошибок могут быть реализованы как на аппаратном уровне, так и на программном. Аппаратный уровень реализации более эффективен. Быстродействие аппаратной реализации протокола MNP примерно на 30% выше, чем программной.

Перечень протоколов MNP

MNP (Microcom Network Protocols) - серия наиболее распространенных аппаратных протоколов, впервые реализованная на модемах фирмы Microcom. Эти протоколы обеспечивают автоматическую коррекцию ошибок и компрессию передаваемых данных.

Сейчас следующие протоколы:

MNP1 . Протокол коррекции ошибок, использующий асинхронный полудуплексный метод передачи данных. Это самый простой из протоколов MNP.

MNP2 . Протокол коррекции ошибок, использующий асинхронный дуплексный метод передачи данных.

MNP3 . Протокол коррекции ошибок, использующий синхронный дуплексный метод передачи данных между модемами (интерфейс модем - компьютер остается асинхронным). Так как при асинхронной передаче используется десять бит на байт - восемь бит данных, стартовый бит и стоповый бит, а при синхронной только восемь, то в этом кроется возможность ускорить обмен данными на 20%.

MNP4 . Протокол, использующий синхронный метод передачи, обеспечивает оптимизацию фазы данных, которая несколько улучшает неэффективность протоколы MNP2 и MNP3. Кроме того, при изменении числа ошибок на линии соответственно меняется и размер блоков передаваемых данных. При увеличении числа ошибок размер блоков уменьшается, увеличивая вероятность успешного прохождения отдельных блоков. Эффективность этого метода составляет около 20% по сравнению с простой передачей данных.

MNP5 . Дополнительно к методам MNP4, MNP5 часто использует простой метод сжатия передаваемой информации. Символы часто встречающиеся в передаваемом блоке кодируются цепочками битов меньшей длины, чем редко встречающиеся символы. Дополнительно кодируются длинные цепочки одинаковых символов. Обычно при этом текстовые файлы сжимаются до 35% своей исходной длины. Вместе с 20% MNP4 это дает повышение эффективности до 50%. Заметим, что если вы передаете уже сжатые файлы, а в большинстве это так и есть, дополнительного увеличения эффективности за счет сжатия данных модемом этого не происходит.

MNP6 . Дополнительно к методам протокола MNP5 автоматически переключается между дуплексным и полудуплексным методами передачи в зависимости от типа информации. Протокол MNP6 также обеспечивает совместимость с протоколом V. 29.

MNP7 . По сравнению с ранними протоколами использует более эффективный метод сжатия данных.

MNP9 . Использует протокол V. 32 и соответствующий метод работы, обеспечивающий совместимость с низкоскоростными модемами.

MNP10 . Предназначен для обеспечения связи на сильно зашумленных линиях, таких, как линии сотовой связи, междугородними линиями, сельские линии. Это достигается при помощи следующих методов:

- многократного повторения попытки установить связь

- изменения размера пакетов в соответствии с изменением уровня помех на линии

- динамического изменения скорости передачи в соответствии с уровнем помех линии

Все протоколы MNP совместимы между собой снизу вверх. При установлении связи происходит установка наивысшего возможного уровня MNP-протокола. Если же один из связывающихся модемов не поддерживает протокол MNP, то MNP-модем работает без MNP-протокола.

Протоколы передачи файлов

В отличие от протоколов нижнего уровня данные протоколы позволяют организовать прием и передачу файлов.

ASCII (American standard code for information interchange). Этот протокол работает без коррекции ошибок. В результате при передаче файлов по телефонным каналам из-за шума принятый файл сильно отличается от передаваемого. Если вы передаете выполняемый файл, то ошибки при передаче могут стать роковыми - полученная программа не будет работать. Если вы передаете короткие текстовые сообщения, то ошибки легко могут быть исправлены.

Xmodem. Наиболее распространены три разновидности протокола Xmodem:

- оригинальный протокол *Xmodem*

- *Xmodem с CRC*

- *1K Xmodem*

Оригинальный протокол ***Xmodem*** разработал Вард Кристенсен (Ward Christensen) в 1977 году. Вард Кристенсен был одним из первых специалистов по протоколам обмена данными. В честь него этот протокол иногда называют также протоколом Кристенсена. При передаче файлов с помощью протоколов Xmodem формат данных должен быть следующим: 8-битовые данные, один стоповый бит и отсутствие проверки на четность. Для передачи используется полудуплексный метод, т. е. данные могут передаваться в каждый момент времени только в одном направлении.

Xmodem Cheksum передает данные пакетами по 128 байт. Вместе с пакетом передается его контрольная сумма. При получении пакета контрольная сумма вычисляется снова и сравнивается с суммой, вычисленной на передающей машине. Пакет передан без ошибок, если суммы совпадают. Этот метод обеспечивает достаточно хорошую защиту от ошибок. Только один из 256 пакетов может содержать ошибки, даже если контрольная сумма правильная.

Xmodem с CRC . Более защищенным от ошибок является протокол Xmodem CRC (Cyclic Redundancy Check). Xmodem CRC - протокол с проверкой циклическим избыточным кодом. В нем 8-битовая контрольная сумма заменена на 16-битовый циклический избыточный код. Этот протокол гарантирует вероятность обнаружения ошибок, равную 99,9984%. Только один из 700 биллионов плохих пакетов будет иметь правильный CRC-код. Протокол Xmodem CRC также передает данные пакетами по 128 байт.

1K Xmodem . Если передача идет без ошибок, протокол 1K Xmodem увеличивает размер пакета с 128 до 1024 байт. При увеличении числа ошибок размер пакета снова уменьшается. Такое изменение длины пакета позволяет

увеличить скорость передачи файлов. В остальном протокол 1K Xmodem совпадает с протоколом Xmodem CRC.

Протокол **Ymodem** разработал Чак Форсберг в 1984-1985 годах. Протокол Ymodem похож на протокол 1K Xmodem, но имеет одно отличие: протокол Ymodem может передавать или принимать за один заход несколько файлов. Существует модификация протокола Ymodem - Ymodem G. Протокол ***Ymodem G*** предназначен для использования с модемами, автоматически осуществляющими коррекцию ошибок на аппаратном уровне. Например, MNP-модемы с аппаратной реализацией MNP. В этом протоколе упрощена защита от ошибок, т. к. ее выполняет сам модем. Не используете этот протокол, если ваш модем не осуществляет аппаратную коррекцию ошибок - данные посылаются сплошным потоком безо всяких стоповых битов си контрольных сумм. Поэтому протокол очень быстрый, но применять его можно только на линиях, абсолютно защищенных от помех. Другой особенностью протокола Ymodem является то, что вместе с файлом передаются все его атрибуты. В результате как минимум имя файла и дата остаются неизменными.

Zmodem - это быстрый протокол передачи данных, использующий окна. Zmodem осуществляет передачу данных пакетами по несколько штук в окне. При этом принимающий данные компьютер не передает сигнал подтверждения или сигнал переспроса неправильного пакета, пока не получит все пакеты в окне. Протокол Zmodem, так же как и протокол 1K Xmodem, может изменять длину пакета (блока) от 64 до 1024 байт в зависимости от качества линии. Кроме того, протокол обладает следующей полезной особенностью: если при передаче файла произошел сбой на линии и вы не успели передать весь файл, то в следующий раз при передаче этого же файла он автоматически начнет передавать с того же места, где произошел обрыв связи. Таким образом, очень большие файлы могут

передаваться по частям. Из всех протоколов верхнего уровня, описанных выше, этот протокол самый быстрый и удобный.

Jmodem использует сжатие данных, а так же изменение длины блока в зависимости от уровня помех - если ошибок много - данные передаются меньшими порциями, и наоборот - при отсутствии ошибок размер одного блока может занимать до 8 Кбайт.

BiModem. Особенностью протокола Bimodem является возможность одновременной передачи двух файлов в разных направлениях. Протокол очень быстрый, позволяет продолжать передачу после обрыва. Кроме того, одновременно с передачей файлов возможна передача сообщений на удаленный компьютер. Недостатком протокола является плохая работа на зашумленных линиях.

Kermit. Широко известны две разновидности протокола Kermit - стандартный и Super Kermit. Этот протокол был разработан в Колумбийском университете в 1981 году для связи между различными типами компьютеров, включая большие компьютеры, мини-компьютеры и персональные компьютеры. В отличие от протоколов Xmodem и Zmodem он использует для передачи данных пакеты переменной длины и максимальным размером 94 байт. Так же как и Ymodem, протокол Kermit может передавать или принимать несколько файлов за один сеанс, одновременно сжимая данные. Коррекция ошибок отличается большей надежностью, чем у Xmodem. Протокол Super Kermit предназначен специально для использования в сетях типа TeleNet или TymNet. Эти сети имеют очень большие задержки при передаче данных. Так что если ждать подтверждения для каждого пакета, это может привести к резкому снижению скорости обмена. В протоколе Super Kermit эта проблема решается следующим способом. Несколько пакетов передается за один раз. Все действия по контролю над ошибками остаются, за исключением того, что принимающий данные компьютер не передает

сигнал подтверждения или сигнал на переспрос неправильного пакета, пока не получит все пакеты в окне. В результате использования такого механизма происходит резкое сокращение времени задержки. Окно может содержать от одного до 31 пакета. В дополнение Kermit использует также предварительную компрессию данных для увеличения эффективной скорости обмена данными. Однако из-за малого размера блоков и большого количества служебной информации эффективность этого протокола крайне низка.

HS/Link - сочетает в себе все достоинства Zmodem, но является бинаправленным, т.е. позволяет обеим сторонам обмениваться файлами - посылать их в обе стороны - одновременно.

Hyper Protocol - один из самых быстрых протоколов. Протокол является потоковым, но помимо того он еще и сжимает посылаемые данные. В Hyper Protocol модем-приемник высылает подтверждение не после каждого файла, а в конце каждого сеанса передачи. Протокол широко применяется на высокоскоростных модемах и на выделенных линиях.

Протоколы передачи данных стандарта CCITT (ITU)

Для разработки стандартов передачи данных был создан специальный Международный консультативный комитет по телеграфии и телефонии (CCITT) (- в 1990 комиссия переименована в ITU- International Telecommunication Union- Международный Телекоммуникационный Союз) и приняты следующие рекомендации:

V.21 - *300 bps* . Модем, регламентированный данной рекомендацией, предназначен для передачи данных по выделенным и коммутируемым линиям. Он работает в асинхронном дуплексном режиме. Для передачи и приема данных используется способ частотной модуляции.

V.22 - *1200 bps* . Модем, работающий в соответствии с данной рекомендацией, использует асинхронно-синхронный дуплексный режим передачи. Асинхронно-синхронный режим означает, что компьютер передает модему данные в асинхронном режиме. Модем удаляет из потока данных компьютера стартовые и стоповые биты. И уже в синхронном виде передает их удаленному компьютеру. Для модуляции передаваемого сигнала применяется метод дифференциальной фазовой модуляции.

V.22bis - *2400 bps* . Дуплексный модем, со скоростью передачи данных 2400 bps. При передаче со скоростью 2400 bps используется метод квадратурной модуляции, а при скорости 1200- метод дифференциальной фазовой модуляции. На скорости 1200bps модем CCITT V. 22bis совместим с CCITT V. 22. Приставка "bis" в переводе с французского означает "второй" - т.е. указывает на вторую разновидность данного протокола.

V.23 - *600/1200 bps*. Асинхронный модем, использующий метод частотной модуляции. Модем может работать в дуплексном режиме со скоростью передачи данных по прямому каналу - 600/1200 bps, а по обратной - только 75 bps. Этот стандарт не совместим с CCITT V. 21, V. 22, V. 22bis.

V.32bis - 14400, 12000, 9600, 7200, 4800 бит/с;

V.32 - 9600, 4800 бит/с;

V.34 - обеспечивает оптимальную производительность (28800 бит/сунда) при работе по любому имеющемуся телефонному каналу. При высоком качестве канала достижима скорость до 33.6 кбит/с (V.34+) (до 128 кбит/с с учетом компрессии).). Искусственно ограничивая звуковой спектр только теми частотами, которые относятся к человеческой речи, сетевые инженеры обнаружили, что они могут сузить необходимую для каждого звонка полосу пропускания, увеличив за счет этого количество возможных одновременных

звонков. И хотя это ограничение хорошо работает для голоса, оно накладывает ограничения на передачу данных.

Модемы V.34 оптимизированы для ситуаций, в которых оба конца подключены к PSTN аналоговыми линиями. И хотя большая часть сети цифровая, модемы V.34 рассматривают ее, как если бы она была полностью аналоговой. Модемы V.34 невероятно устойчивы, но они не могут воспринять всю полосу пропускания, которая становится доступной в том случае, если один из концов соединения будет полностью цифровым. Стандарт V.34 был построен на предположении, что оба конца соединения несут ущерб от шума квантования, появляющегося вследствие использования аналого-цифровых преобразователей (analog-to-digital converters - ADC).

V.42 и **V.42bis** - протокол с коррекцией ошибок и преобразованием асинхронный синхронный. Протокол использует метод компрессии, при котором определяется частота появления отдельных символьных строк и происходит их замена на последовательности символов меньшей длины. Этот метод компрессии носит название Lempel-Ziv. Данный метод компрессии обеспечивает 50% сжатие текстовых файлов. Вместе с 20% выигрышем от синхронного преобразования это увеличивает эффективность на 60%.

V.90- технология передачи данных, разработанная Study Group 16 Международного Телекоммуникационного Союза - предлагает спецификацию для достижения скоростей в линии до 56 Кбит/с. V.90 за счет использования цифровых соединений с сервером, используемых большинством провайдеров Internet и онлайновых услуг для подключения к PSTN (телефонной линии) "на своем конце", преодолевает теоретические ограничения, накладываемые на стандартные аналоговые модемы (физическая сторона вопроса рассмотрена в Разделе 4).

x2 компании 3Com/US Robotics позволяет передавать данные со скоростью 56 Кбит в секунду.

K56flex - аналогичный стандарт, предложенный совместно фирмами Lucent и Rockwell.

V.com -альтернативная двум предыдущим технология, позволяющая осуществлять совместное использование устройств US Robotics, Lucent и Rockwell.

В феврале 1998 года ITU добился определения технологии доступа на 56 Кбит/с, предложив единое универсально совместимое решение - стандарт V.90. Решение V.90 корпорации 3Com остается совместимым с собственной схемой корпорации 3Com передачи для доступа на 56 Кбит/с - технологией x2.

2. FAX-протоколы

Факс-протоколы модуляции.

Протоколы V.27, V.27bis, V.27ter. Из протоколов V.27, V.27bis, V.27ter два первых предназначены для использования на четырехпроводных выделенных линиях, а V.27ter - на двухпроводных коммутируемых каналах связи. В протоколах применяется относительная фазовая модуляция с частотой несущей 1800 Гц. Возможна работа на скоростях 2400 и 4800 бит/с. Протокол V.27bis позволяет организовать полнодуплексную передачу на четырехпроводных линиях и полудуплексную на телефонных каналах с двухпроводным окончанием. Протокол V.27ter предусматривает использование автоматического адаптивного корректора.

Протокол V.29. Протокол V.29 предусматривает возможность работы со скоростями 9600, 7200 и 4800 бит/с по четырехпроводным выделенным телефонным каналам. Частота несущей равна 1700 Гц, а скорость модуляции

- 2400 Бод. Применена квадратурная амплитудная модуляция. Данный протокол предусматривает возможность многоканальной передачи, то есть можно организовать передачу по четырем каналам со скоростью 2400 бит/с.

Протокол V.17. Протокол V.17 является самым скоростным факс-протоколом модуляции. По своим параметрам он похож на V.32bis. Частота несущей 1800 ГЦ, а скорость модуляции - 2400 Бод. Информационная скорость передачи может быть 7200, 9600, 12000 и 14400 бит/с.

3. Протоколы локальных сетей физического уровня: Ethernet, ARCnet, Token Ring.

Технология Ethernet

Ethernet - это самый распространенный на сегодняшний день стандарт локальных сетей. Общее количество сетей, работающих по протоколу Ethernet в настоящее время, оценивается в 5 миллионов, а количество компьютеров с установленными сетевыми адаптерами Ethernet - в 50 миллионов.

Когда говорят Ethernet, то под этим обычно понимают любой из вариантов этой технологии. В более узком смысле *Ethernet - это сетевой стандарт*, основанный на экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году. Метод доступа был опробован еще раньше: во второй половине 60-х годов в радиосети Гавайского университета использовались различные варианты случайного доступа к общей радиосреде, получившие общее название Aloha. В 1980 году фирмы DEC, Intel и Xerox совместно разработали и опубликовали стандарт Ethernet версии II для сети, построенной на основе коаксиального кабеля, который стал последней версией фирменного стандарта Ethernet. Поэтому фирменную версию стандарта Ethernet называют стандартом Ethernet DIX или Ethernet II.

На основе стандарта *Ethernet DIX* был разработан стандарт *IEEE 802.3*, который во многом совпадает со своим предшественником, но некоторые различия все же имеются. В то время как в стандарте *IEEE 802.3* различаются уровни MAC и LLC, в оригинальном Ethernet оба эти уровня объединены в единый канальный уровень, В Ethernet DIX определяется протокол тестирования конфигурации (*Ethernet Configuration Test Protocol*), который отсутствует в *IEEE 802.3*. Несколько отличается и формат кадра, хотя минимальные и максимальные размеры кадров в этих стандартах совпадают. Часто для того, чтобы отличить Ethernet, определенный стандартом IEEE, и фирменный Ethernet DIX, первый называют технологией 802.3, а за фирменным оставляют название Ethernet без дополнительных обозначений.

В зависимости от типа физической среды стандарт IEEE 802.3 имеет различные модификации -

- *10Base-5,*
- *10Base-2,*
- *10Base-T,*
- *10Base-FL,*
- *10Base-FB*

В 1995 году был принят стандарт Fast Ethernet, который во многом не является самостоятельным стандартом, о чем говорит и тот факт, что его описание просто является дополнительным разделом к основному стандарту 802,3 - разделом 802.3ч. Аналогично, принятый в 1998 году стандарт Gigabit Ethernet описан в разделе 802.3z основного документа.

Для передачи двоичной информации по кабелю для всех вариантов физического уровня технологии Ethernet, обеспечивающих пропускную способность 10 Мбит/с, используется манчестерский код.

Все виды стандартов Ethernet (в том числе Fast Ethernet и Gigabit Ethernet) используют один и тот же метод разделения среды передачи данных - метод CSMA/CD.

Спецификации физической среды Ethernet

Исторически первые сети технологии Ethernet были созданы на коаксиальном кабеле диаметром 0,5 дюйма. В дальнейшем были определены и другие спецификации физического уровня для стандарта Ethernet, позволяющие использовать различные среды передачи данных. Метод доступа CSMA/CD и все временные параметры остаются одними и теми же для любой спецификации физической среды технологии Ethernet 10 Мбит/с.

Физические спецификации технологии Ethernet на сегодняшний день включают следующие среды передачи данных.

- **10Base-5** - коаксиальный кабель диаметром 0,5 дюйма, называемый «толстым» коаксиалом. Имеет волновое сопротивление 50 Ом. Максимальная длина сегмента - 500 метров (без повторителей).
- **10Base-2** - коаксиальный кабель диаметром 0,25 дюйма, называемый «тонким» коаксиалом. Имеет волновое сопротивление 50 Ом. Максимальная длина сегмента - 185 метров (без повторителей).
- **10Base-T** - кабель на основе неэкранированной витой пары (Unshielded Twisted Pair, UTP). Образует звездообразную топологию на основе концентратора. Расстояние между концентратором и конечным узлом - не более 100 м.
- **10Base-F** - волоконно-оптический кабель. Топология аналогична топологии стандарта 10Base-T. Имеется несколько вариантов этой спецификации - FOIRL (расстояние до 1000 м), 10Base-FL (расстояние до 2000 м), 10Base-FB (расстояние до 2000 м).

Число 10 в указанных выше названиях обозначает битовую скорость передачи данных этих стандартов - 10 Мбит/с, *Слово Base* - метод передачи на одной базовой частоте 10 МГц (в отличие от методов, использующих несколько несущих частот, которые называются Broadband - широкополосными). Последний символ в названии стандарта физического уровня обозначает тип кабеля.

Технология Token Ring (802.5)

Основные характеристики технологии

Сети Token Ring, так же как и сети Ethernet, характеризует разделяемая среда передачи данных, которая в данном случае состоит из отрезков кабеля, соединяющих все станции сети в кольцо. Кольцо рассматривается как общий разделяемый ресурс, и для доступа к нему требуется не случайный алгоритм, как в сетях Ethernet, а детерминированный, основанный на передаче станциям права на использование кольца в определенном порядке. Это право передается с помощью кадра специального формата, называемого *маркером* или *токеном (token)*.

Технология Token Ring был разработана компанией IBM в 1984 году, а затем передана в качестве проекта стандарта в комитет IEEE 802, который на ее основе принял в 1985 году стандарт 802.5. Компания IBM использует технологию Token Ring в качестве своей основной сетевой технологии для построения локальных сетей на основе компьютеров различных классов - мэйнфреймов, мини-компьютеров и персональных компьютеров. В настоящее время именно компания IBM является основным законодателем моды технологии Token Ring, производя около 60 % сетевых адаптеров этой технологии.

Сети Token Ring работают с двумя битовыми скоростями - 4 и 16 Мбит/с. Смешение станций, работающих на различных скоростях, в одном кольце не

допускается. Сети Token Ring, работающие со скоростью 16 Мбит/с, имеют некоторые усовершенствования в алгоритме доступа по сравнению со стандартом 4 Мбит/с.

Технология Token Ring является более сложной технологией, чем Ethernet. Она обладает свойствами отказоустойчивости. В сети Token Ring определены процедуры контроля работы сети, которые используют обратную связь кольцеобразной структуры - посланный кадр всегда возвращается в станцию - отправитель. В некоторых случаях обнаруженные ошибки в работе сети устраняются автоматически, например может быть восстановлен потерянный маркер. В других случаях ошибки только фиксируются, а их устранение выполняется вручную обслуживающим персоналом.

Для контроля сети одна из станций выполняет роль так называемого *активного монитора*. Активный монитор выбирается во время инициализации кольца как станция с максимальным значением MAC-адреса, Если активный монитор выходит из строя, процедура инициализации кольца повторяется и выбирается новый активный монитор. Чтобы сеть могла обнаружить отказ активного монитора, последний в работоспособном состоянии каждые 3 секунды генерирует специальный кадр своего присутствия. Если этот кадр не появляется в сети более 7 секунд, то остальные станции сети начинают процедуру выборов нового активного монитора.

Маркерный метод доступа к разделяемой среде

В сетях с *маркерным методом доступа* (а к ним, кроме сетей Token Ring, относятся сети FDDI, а также сети, близкие к стандарту 802.4, - ArcNet, сети производственного назначения MAP) право на доступ к среде передается циклически от станции к станции по логическому кольцу.

В сети Token Ring кольцо образуется отрезками кабеля, соединяющими соседние станции. Таким образом, каждая станция связана со своей предшествующей и последующей станцией и может непосредственно обмениваться данными только с ними. Для обеспечения доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения - маркер. В сети Token Ring любая станция всегда непосредственно получает данные только от одной станции - той, которая является предыдущей в кольце. Такая станция называется *ближайшим активным соседом, расположенным выше по потоку* (данных) - *Nearest Active Upstream Neighbor, NAUN*. Передачу же данных станция всегда осуществляет своему ближайшему соседу вниз по потоку данных.

Получив маркер, станция анализирует его и при отсутствии у нее данных для передачи обеспечивает его продвижение к следующей станции. Станция, которая имеет данные для передачи, при получении маркера изымает его из кольца, что дает ей право доступа к физической среде и передачи своих данных. Затем эта станция выдает в кольцо кадр данных установленного формата последовательно по битам. Переданные данные проходят по кольцу всегда в одном направлении от одной станции к другой. Кадр снабжен адресом назначения и адресом источника.

Все станции кольца ретранслируют кадр побитно, как повторители. Если кадр проходит через станцию назначения, то, распознав свой адрес, эта станция копирует кадр в свой внутренний буфер и вставляет в кадр признак подтверждения приема. Станция, выдавшая кадр данных в кольцо, при обратном его получении с подтверждением приема изымает этот кадр из кольца и передает в сеть новый маркер для обеспечения возможности другим станциям сети передавать данные. Такой алгоритм доступа применяется в сетях Token Ring со скоростью работы 4 Мбит/с, описанных в стандарте 802.5.

На (рис. 3.9) описанный алгоритм доступа к среде иллюстрируется временной диаграммой. Здесь показана передача пакета А в кольце, состоящем из 6 станций, от станции *1* к станции *3*. После прохождения станции назначения *3* в пакете А устанавливаются два признака - признак распознавания адреса и признак копирования пакета в буфер (что на рисунке отмечено звездочкой внутри пакета). После возвращения пакета в станцию *1* отправитель распознает свой пакет по адресу источника и удаляет пакет из кольца. Установленные станцией *3* признаки говорят станции-отправителю о том, что пакет дошел до адресата и был успешно скопирован им в свой буфер.

Время владения разделяемой средой в сети Token Ring ограничивается *временем удержания маркера (token holding time)*, после истечения которого станция обязана прекратить передачу собственных данных (текущий кадр разрешается завершить) и передать маркер далее по кольцу. Станция может успеть передать за время удержания маркера один или несколько кадров в зависимости от размера кадров и величины времени удержания маркера. Обычно время удержания маркера по умолчанию равно 10 мс, а максимальный размер кадра в стандарте 802.5 не определен. Для сетей 4 Мбит/с он обычно равен 4 Кбайт, а для сетей 16 Мбит/с - 16 Кбайт. Это связано с тем, что за время удержания маркера станция должна успеть передать хотя бы один кадр. При скорости 4 Мбит/с за время 10 мс можно передать 5000 байт, а при скорости 16 Мбит/с - соответственно 20 000 байт. Максимальные размеры кадра выбраны с некоторым запасом.

В сетях Token Ring 16 Мбит/с используется также несколько другой алгоритм доступа к кольцу, называемый алгоритмом *раннего освобождения маркера (Early Token Release)*. В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема. В этом случае пропускная способность кольца

используется более эффективно, так как по кольцу одновременно продвигаются кадры нескольких станций. Тем не менее свои кадры в каждый момент времени может генерировать только одна станция - та, которая в данный момент владеет маркером доступа. Остальные станции в это время только повторяют чужие кадры, так что принцип разделения кольца во времени сохраняется, ускоряется только процедура передачи владения кольцом.

Для различных видов сообщений, передаваемым кадрам, могут назначаться различные *приоритеты*: от 0 (низший) до 7 (высший). Решение о приоритете конкретного кадра принимает передающая станция (протокол Token Ring получает этот параметр через межуровневые интерфейсы от протоколов верхнего уровня, например прикладного). Маркер также всегда имеет некоторый уровень текущего приоритета. Станция имеет право захватить переданный ей маркер только в том случае, если приоритет кадра, который она хочет передать, выше (или равен) приоритета маркера. В противном случае станция обязана передать маркер следующей по кольцу станции.

За наличие в сети маркера, причем единственной его копии, отвечает активный монитор. Если активный монитор не получает маркер в течение длительного времени (например, 2,6 с), то он порождает новый маркер.

Форматы кадров Token Ring

В Token Ring существуют три различных формата кадров:

- маркер;
- кадр данных;
- прерывающая последовательность.

Первыми технологиями построения ЛВС, получившими коммерческое признание, были патентованные решения **ARCNET**(*Attached Resource Computer NETwork*) и**Token**

ring(маркерное кольцо), однако в начале 90-х годов прошлого века они постепенно были практически повсеместно вытеснены сетями на базе семейства протоколов**Ethernet**.

Этот протокол был разработан Исследовательским центром в Пало Альто (PARC) корпорации Xerox в 1973-м году. В 1980 компании Digital Equipment Corporation, Intel Corporation и Xerox Corporation совместно разработали и приняли спецификацию Ethernet (Version 2.0). Тогда же в институте IEEE (Institute of Electrical and Electronics Engineers) был организован комитет 802 по стандартизации локальных сетей, в результате работы которого было принято семейство стандартов IEEE 802.x, которые содержат рекомендации по проектированию нижних уровней локальных сетей. В это семейство входят несколько групп стандартов:

802.1 — объединение сетей.

802.2 — Управление логической связью.

802.3 — ЛВС с множественным доступом, контролем несущей и обнаружением коллизий (Ethernet).

802.4 — ЛВС топологии «шина» с передачей маркера.

802.5 — ЛВС топологии «кольцо» с передачей маркера.

802.6 — сеть масштаба города (Metropolitan Area Network, MAN).

802.7 — Консультативный совет по широковещательной технологии (Broadcast Technical Advisory Group).

802.8 -- Консультативный совет по оптоволоконной технологии (Fiber-Optic Technical Advisory Group).

802.9 — Интегрированные сети с передачей речи и данных (Integrated Voice/Data Networks).

802.10 — Безопасность сетей.

802.11 — Беспроводная сеть.

802.12 — ЛВС с доступом по приоритету запроса (Demand Priority Access LAN,

lOObaseVG-AnyLan).

802.13 – номер не был использован !!!

802.14 – Передача данных по сетям кабельного TV (не активна с 2000 г.)

802.15 - Беспроводные персональные сети (WPAN) например Bluetooth, ZigBee, 6loWPAN

802.16 - Беспроводные сети WiMAX (*Worldwide Interoperability for Microwave Access*, по-русски читается*ваймáкс*)

802.17 называется RPR (Resilient Packet Ring - адаптивное кольцо для пакетов). Разрабатывается с 2000 года в качестве современной магистральной сети городского масштаба.

По каждой группе работает свой подкомитет, который разрабатывает и принимает обновления. Стандарты серии IEEE 802 охватывают два уровня модели OSI, нас пока интересуют только те из них и в той части, которые описывают физический уровень.

1.5 Лекция № 8 (2 часа).

Тема: «Безопасность в вычислительных сетях**»**

1.5.1 Вопросы лекции:

1) Аппаратные и программные средства защиты информации

2) Криптография

3) Шифрование с секретными ключами

4) Шифрование с открытыми ключами

1.5.2 Краткое содержание вопросов:

1. Аппаратные и программные средства защиты информации

Несмотря на то, что современные ОС для персональных компьютеров, такие, как Windows 2000, Windows XP и Windows NT, имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты сохраняется. Дело в том, что большинство систем не способны защитить данные, находящиеся за их пределами, например при сетевом информационном обмене.

Аппаратно-программные средства защиты информации можно разбить на пять групп:

1. Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.
2. Системы шифрования дисковых данных.
3. Системы шифрования данных, передаваемых по сетям.
4. Системы аутентификации электронных данных.

5. Средства управления криптографическими ключами.

1. Системы идентификации и аутентификации пользователей

Применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы. Общий алгоритм работы таких систем заключается в том, чтобы получить от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

При построении этих систем возникает проблема выбора информации, на основе которой осуществляются процедуры идентификации и аутентификации пользователя. Можно выделить следующие типы:

- секретная информация, которой обладает пользователь (пароль, секретный ключ, персональный идентификатор и т.п.); пользователь должен запомнить эту информацию или же для нее могут быть применены специальные средства хранения;
- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на клавиатуре и т.п.).

Системы, основанные на первом типе информации, считаются ***традиционными***. Системы, использующие второй тип информации, называют ***биометрическими***. Следует отметить наметившуюся тенденцию опережающего развития биометрических систем идентификации.

2. Системы шифрования дисковых данных

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая ***криптографией*** [от греч. ***kryptos***- скрытый и ***grapho*** - пишу].

Системы шифрования могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков. К программам первого типа можно отнести архиваторы типа ARJ и RAR, которые позволяют использовать криптографические методы для защиты архивных файлов. Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities, Best Crypt.

Другим классификационным признаком систем шифрования дисковых данных является способ их функционирования. По способу функционирования системы шифрования дисковых данных делят на два класса:

- системы "прозрачного" шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах прозрачного шифрования (шифрования "на лету") криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

Системы второго класса обычно представляют собой утилиты, которые необходимо специально вызывать для выполнения шифрования. К ним относятся, например, архиваторы со встроенными средствами парольной защиты.

Большинство систем, предлагающих установить пароль на документ, не шифрует информацию, а только обеспечивает запрос пароля при доступе к документу. К таким системам относится MS Office, 1С и многие другие.

3. Системы шифрования данных, передаваемых по сетям

Различают два основных способа шифрования: канальное шифрование и оконечное (абонентское) шифрование.

В случае ***канального шифрования*** защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством - встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы. Однако у данного подхода имеются и существенные недостатки:

- шифрование служебных данных осложняет механизм маршрутизации сетевых пакетов и требует расшифрования данных в устройствах промежуточной коммуникации (шлюзах, ретрансляторах и т.п.);
- шифрование служебной информации может привести к появлению статистических закономерностей в шифрованных данных, что влияет на надежность защиты и накладывает ограничения на использование криптографических алгоритмов.

Оконечное (абонентское) шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами. В этом случае защищается только содержание сообщений, вся служебная информация остается открытой. Недостатком является возможность анализировать информацию о структуре обмена сообщениями, например об отправителе и получателе, о времени и условиях передачи данных, а также об объеме передаваемых данных.

4. Системы аутентификации электронных данных

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для

аутентификации данных применяют код аутентификации сообщения (имитовставку) или электронную подпись.

Имитовставка вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных. Имитовставка проверяется получателем, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными.

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Таким образом, для реализации имитовставки используются принципы симметричного шифрования, а для реализации электронной подписи - асимметричного. Подробнее эти две системы шифрования будем изучать позже.

5. Средства управления криптографическими ключами

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети.

Различают следующие виды функций управления ключами: генерация, хранение, и распределение ключей.

Способы ***генерации ключей*** для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем

используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами. Подробнее на этом вопросе остановимся при изучении симметричных и асимметричных криптосистем.

Функция ***хранения*** предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ (т.е. мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключа является критическим вопросом криптозащиты.

Распределение - самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным. Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.

2. Криптография

Криптография (от греч. κρυπτός — скрытый и γράφω — писать) – древнейшая наука о способах защиты конфиденциальных данных от нежелательного стороннего прочтения. Криптоанализ – наука, изучающая методы нарушения конфиденциальности информации. Криптанализ и криптография вместе составляют науку криптологию, изучающую способы шифрования и дешифрования.

Криптография является древнейшей наукой, и первоначальными ее объектами были текстовые сообщения, которые с помощью определенных

алгоритмов лишались смысла для всех, не обладающих специальным знанием по дешифровке этого сообщения – ключом.

Изначально использовались методы, сегодня применяемые разве что для головоломок, то есть, на взгляд современника, простейшие. К таким способам шифрования относятся, например, метод замены, когда каждая буква заменяется другой, отстоящей от нее на строго определенном расстоянии в алфавите. Или метод перестановочного шифрования, когда буквы меняют местами в определенной последовательности внутри слова.

В древние времена шифрование применялось главным образом в военном и торговом деле, шпионаже, среди контрабандистов.

Несколько позже ученые-историки определяют дату появления другой родственной науки – стеганография. Эта наука занимается маскировкой самого факта передачи сообщения. Зародилась она в античности, а примером здесь может служить получение спартанским царем Леонидом перед битвой с персами провощенной дощечки с текстом, покрытой сухим легкосмываемым раствором. При очистке оставленные на воске стилусом знаки становились отчетливо видимыми. Сегодня для сокрытия сообщения служат симпатические чернила, микроточки, микропленки и т.д.

С развитием математики стали появляться математические алгоритмы шифрования, но все эти виды криптографической защиты информации сохраняли в разной объемной степени статистические данные и оставались уязвимыми. Уязвимость стала особенно ощутима с изобретением частотного анализа, который был разработан в IX веке нашей эры предположительно арабским энциклопедистом ал-Кинди. И только в XV веке, после изобретения полиалфавитных шрифтов Леоном Баттистой Альберти (предположительно), защита перешла на качественно новый уровень. Однако в середине XVII века Чарлз Бэббидж представил убедительные доказательства частичной уязвимости полиалфавитных шрифтов перед частотным анализом.

Развитие механики позволило создавать приборы и механизмы, облегчающие шифрование – появились такие устройства, как квадратная доска Тритемиуса, дисковый шифр Томаса Джефферсона. Но все эти приборы ри в какое сравнение не идут с теми, были созданы в XX веке. Именно в это время стали появляться различные шифровальные машины и механизмы высокой сложности, например, роторные машины, самой известной из которых является «Энигма»

До бурного развития науки в XX веке криптографам приходилось иметь дело только с лингвистическими объектами, а в XX веке открылись возможности применения различных математических методов и теорий, статистики, комбинаторики, теории чисел и абстракной алгебры.

Но настоящий прорыв в криптографической науке произошел с появлением возможности представления любой информации в бинарном виде, разделенной на биты с помощью компьютеров, что позволило создавать шрифты с доселе невиданной криптографической стойкостью. Такие системы шифрования, конечно, могут быть подвергнуты взлому, но временные затраты на взлом себя в подавляющем большинстве случаев не оправдывают.

Сегодня можно говорить о значительных разработках в квантовой криптографии.

3.Шифрование с секретными ключами

Шифрование с секретным ключом

Существует два основных типа шифрования: с секретным ключом и с открытым ключом. При шифровании с секретным ключом требуется, чтобы все стороны, имеющие право на прочтение информации, имели один и тот же *ключ*. Это позволяет свести общую проблему безопасности информации к проблеме обеспечения защиты ключа. *Шифрование* с открытым ключом

является наиболее широко используемым методом шифрования. Он обеспечивает *конфиденциальность* информации и гарантию того, что *информация*остается неизменной в процессе передачи.

В чем суть шифрования на секретном ключе?

Шифрование на секретном ключе также называется симметричным шифрованием, так как для шифрования и дешифрования данных используется один и тот же *ключ*. На рисунке 12.2 показан базовый принцип шифрования с секретным ключом. Как видно из рисунка, отправитель и получатель информации должны иметь одинаковый *ключ*.

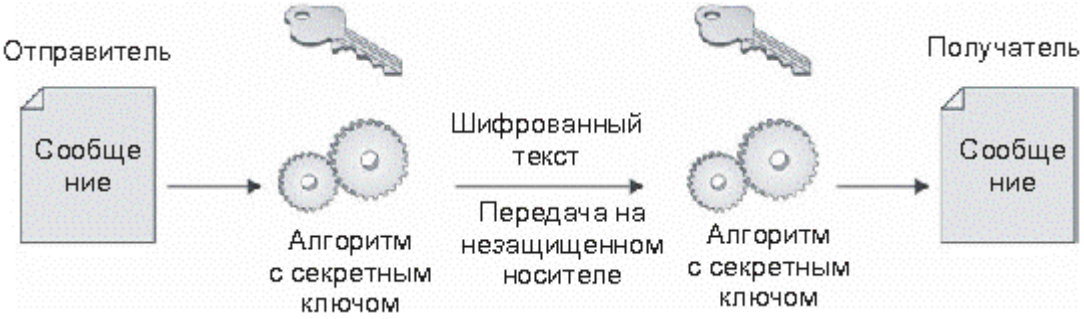


Рис. 12.2. Шифрование с секретным ключом

Шифрование с секретным ключом обеспечивает *конфиденциальность* информации в зашифрованном состоянии. Расшифровать сообщение могут только те лица, которым известен *ключ*. Любое изменение в сообщении, внесенное во время передачи, будет обнаружено, так как после этого не удастся правильно расшифровать сообщение. *Шифрование* с секретным ключом не обеспечивает аутентификацию, поскольку любой *пользователь* может создавать, шифровать и отправлять действительное сообщение.

В общем, *шифрование* с секретным ключом быстро и легко реализуется с помощью аппаратных или программных средств.

Подстановочные шифры

Подстановочные шифры существуют уже около 2500 лет. Самым ранним примером является *шифр* Атбаш. Он возник примерно в 600 году до н.э. и заключался в использовании еврейского алфавита в обратном порядке.

Юлий Цезарь использовал подстановочный *шифр*, который так и назывался - *шифр* Цезаря. Этот *шифр* заключался в замещении каждой буквы другой буквой, расположенной в алфавите на три буквы дальше от шифруемой. Таким образом, буква A преобразовывалась в D, B преобразовывалась в E, а Z преобразовывалась в C.

Из этого примера видно, что подстановочный *шифр* обрабатывает за один раз одну букву *открытого текста*. Сообщение может быть прочитано обоими абонентами при использовании одной и той же схемы подстановки. Ключом в шифре подстановки является либо число букв сдвига, либо полностью переупорядоченный *алфавит*.

Подстановочные шифры имеют один большой недостаток - неизменная частота букв в исходном алфавите. В английском языке, например, буква "E" является наиболее часто используемой. Если заменить ее другой буквой, то чаще всего будет использоваться новая буква (при рассмотрении большого числа сообщений). При помощи такого анализа подстановочный *шифр* может быть взломан. Дальнейшая разработка анализа частоты вхождений букв позволяет получить наиболее часто встречающиеся комбинации из двух и трех букв. С помощью такого анализа можно взломать любой подстановочный *шифр*, если атакующий получит достаточное количество шифрованного текста.

Одноразовые блокноты

Одноразовые блокноты (One-*time Pad*, *OTP*) являются единственной теоретически невзламываемой системой шифрования. Одноразовый блокнот представляет собой *список* чисел в случайном порядке, используемый для кодирования сообщения (см. табл. 12.1). Как видно из названия системы, *OTP* может использоваться только один раз. Если числа в *OTP* являются действительно случайными, *OTP* имеет большую длину, чем сообщение, и используется только один раз, то шифрованный текст не предоставляет какого-либо механизма для восстановления исходного ключа (т. е. самого *OTP*) и, следовательно, сообщений.

Одноразовые блокноты используются в информационных средах с очень высоким уровнем безопасности (но только для коротких сообщений). Например, в Советском Союзе *OTP* использовался для связи разведчиков с Москвой. Двумя основными недостатками*OTP* являются генерация действительно случайных блокнотов и проблема распространения блокнотов. Очевидно, что если блокнот выявляется, то раскрывается и та *информация*, которую он защищает. Если блокноты не являются действительно случайными, могут быть выявлены схемы, которые можно использовать для проведения анализа частоты встречаемых символов.

Таблица 12.1. Функционирование одноразового блокнота

Сообщение	S E N DH EL P
Буквы, замененные соответствующими числами	195 144 8 5 1216
Одноразовый блокнот	7 9 5 2 1210 6
Добавление *открытого текста* в OTP	2614196 206 1222
Шифрованный текст	Z N S F T FL V

Еще одним важным моментом, связанным с *OTP*, является то, что одноразовые блокноты могут использоваться только один раз.

Если *OTP* используется несколько раз, то его можно проанализировать и взломать. Это происходило с некоторыми советскими *OTP*в период холодной войны. Тогда для считывания зашифрованной информации в Национальном Агентстве безопасности был создан проект "*Верона*". *Информация* о *перехватах данных* этим проектом находится на сайте *NSA* (http://www.nsa.gov).

Внимание!

Некоторые современные системы шифрования также используют что-то вроде *OTP*. Этот тип систем шифрования обеспечивает достаточно высокий уровень защиты, однако он точно также является легко взламываемой системой. Как правило, *OTP* непригодны для использования в средах с большим объемом трафика.

4.Шифрование с открытыми ключами

В алгоритмах шифрования с открытым ключом используются два ключа. Один ключ – при шифровании информации, другой – при дешифровке.

Шифрование с открытым ключом

Оба абонента (и отправитель, и получатель) должны иметь ключ. Ключи связаны друг с другом (поэтому они называются парой ключей), но они различны. Т.е., если сообщение зашифровано с помощью ключа К1, то расшифровать это сообщение можно только с помощью ключа К2. И наоборот. При этом один ключ называют секретным, а другой – открытым. Секретный ключ содержится в тайне владельцем пары ключей. Открытый ключ передается вместе с информацией в открытом виде, т.к. у абонента имеется один из ключей пары, а другой ключ вычислить просто невозможно.

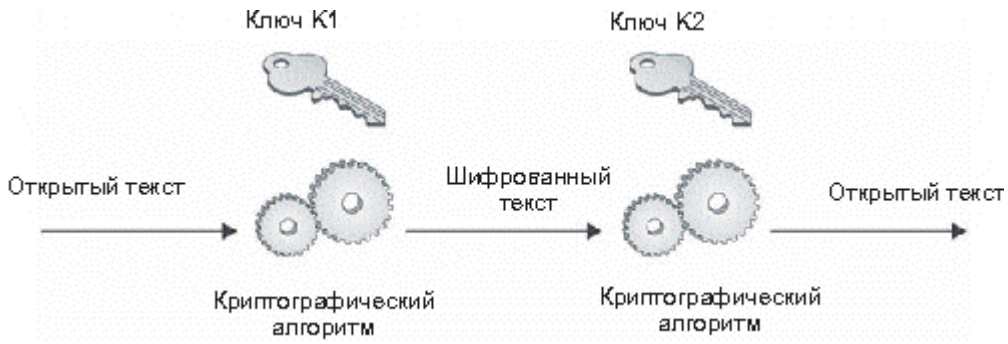


Рис. 7. Шифрование с открытым ключом

Для конфиденциальности, шифрование выполняется с открытым ключом. Тогда расшифровать информацию может только владелец ключа, так как секретный ключ содержится в тайне самим владельцем. Если исходная информация была зашифрована с помощью секретного ключа владельца, то Целостность информации после передачи может быть проверена. Недостаток: систем шифрования с открытым ключом требуют больших вычислительных мощностей, а значит, являются намного менее быстродействующими, нежели системы с секретным ключом.

Алгоритм обмена ключами Диффи-Хеллмана Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin Hellman) разработали свою систему шифрования с открытым ключом в 1976 г. Система Диффи-Хеллмана (Diffie-Hellman) разрабатывалась для решения проблемы распространения ключей при использовании систем шифрования с секретными ключами. Идея заключалась в том, чтобы применять безопасный метод согласования секретного ключа без передачи ключа каким-либо другим способом. Следовательно, необходимо было найти безопасный способ получения секретного ключа с помощью того же метода связи, для которого разрабатывалась защита. Алгоритм Диффи-Хеллмана нельзя использовать для шифрования или дешифрования информации. Работа алгоритма Диффи-Хеллмана

Два абонентам (P1 и P2) согласовывают ключ шифрования для установки между собой безопасного соединения.

P1 и P2 используют два больших целых числа a и b, причем $1 < a < b$.

P1 выбирает случайное число i и вычисляет $I = a^i \bmod b$, и передает I абоненту P2.

P2 выбирает случайное число j и вычисляет $J = a^j \bmod b$, и передает J абоненту P1.

P1 вычисляет $k1 = J^i \bmod b$.

P2 вычисляет $k2 = I^j \bmod b$.

Имеем $k1 = k2 = a^{i*j} \bmod b$. Отсюда вывод, k1 и k2 являются секретными ключами, предназначенными для использования при передаче других данных.
Разъяснение алгоритма Диффи-Хеллмана: «mod» – это остаток. Например, $12 \bmod 10 = 2$. Два – это остаток от деления 12 на 10.
При прослушивании злоумышленником трафика, передаваемого по кабелю, ему станут известны a, b, I и J. Тем не менее, остаются в секрете i и j. Чем будет сложнее нахождение i при известном $I = a^i \bmod b$, тем выше уровень безопасности. Эта задача называется задачей дискретного логарифмирования и считается очень сложной (т. е. с помощью современного вычислительного оборудования ее решить практически невозможно), если числа очень велики. Следовательно, a и bнеобходимо выбирать очень тщательно, и оба числа b и $(b – 1)/2$ должны быть простыми и иметь длину не менее 512 бит, а лучше 1024 бит.

Недостаток: она может быть уязвима для атаки посредником. Другими словами, при размещении злоумышленником своего компьютера между абонентами P1 и P2, подключить его к каналу связи и осуществлять перехват всей передаваемой информации, то он сможет выполнять обмен данными

с P2, выдавая себя за P1, и с P1 под видом P2. Осуществление такой атаки требует большого объема ресурсов, и в реальном мире такие атаки происходят редко.
Алгоритм RSA Rivest-Shamir-Adleman (RSA) с открытым ключом, используется для шифрования и дешифрования. Базовый алгоритм, позволяющий обеспечить конфиденциальность данных: Шифрованный текст = (открытый текст)e mod n Открытый текст = (шифрованный текст)d mod n Секретный ключ = {d, n} Открытый ключ = {e, n}

Безопасность обеспечивается сложностью вычисления d при наличии известных e и n, т.е. владелец пары ключей сохраняет секретный ключ в тайне, и что открытый ключ передается в открытом виде. Следовательно, при зашифровке с помощью открытого ключа, дешифровать ее может только владелец ключевой пары. Для обеспечения аутентификации отправителя алгоритм приобретет следующий вид. Шифрованный текст = (открытый текст)d mod n Открытый текст = (шифрованный текст)e mod n Секретный ключ = {d, n} Открытый ключ = {e, n} Для аутентификации информация шифруется с использованием секретного ключа. Любое лицо может дешифровать информацию и удостовериться в том, что данные поступили именно от владельца ключевой пары.

Генерация ключей RSA

Выбераются и содержатся в секрете два простых числа p и q.

Вычисляем n = pq.

Вычисляем ϕ(n) = (p – 1)(q – 1).

Выбераем такое e, чтобы оно было взаимно простым по отношению к ϕ(n).

Определяем такое d, чтобы (d)(e) = 1 mod ϕ(n) и d < ϕ(n).

Пример с легко проверяемыми числами.

Выбраны числа p = 11 и q = 13.

вычисляем n = pq. Имеем n = 11 x 13 = 143.

Вычисляем ф(n) = (p – 1)(q – 1) = (11 – 1)(13 – 1) = 10 x 12 = 120.

Выбираем число e так, чтобы оно было простым относительно ф(n). Здесь было выбрано значение e = 7.

Необходимо определить такое d, чтобы (d)(e) = 1 mod ф(n). Следовательно, (d)(7) = 1 mod 120; d должно также быть меньше 120. Находим, что d = 103. (103 умножаем на 7 и получается 721. 721 делим на 120 и получаем 6 с остатком 1.)

Секретный ключ: {103, 143}.

Открытый ключ: {7, 143}.

Для выполнения непосредственно шифрования и дешифрования используем исходные формулы.

Шифрованный текст = (открытый текст)e mod n Открытый текст = (шифрованный текст)d mod n Предположим, что нужно отправить сообщение "9″.Шифрованный текст = (9)7 mod 143 = 48. При получении нформация дешифруется: Открытый текст = (48)103 mod 143 = 9.

2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

2.1 Практическое занятие № 1, 2, 3 (6 часов).

Тема: «Оргтехника и другие электронные устройства»

2.1.1 Задание для работы:

1) Сканер и системы распознавания текста

2) Факсимильная связь

3) Копировальные аппараты

2.1.2 Краткое описание проводимого занятия:

Современные средства оргтехники делятся в зависимости от области предназначения на: 1. Коммуникационные. Сюда относятся средства телефонной, мобильной, факсимильной связи, а также электронная почта. По расположению телефоны делятся на носимые и стационарные, а по системам связи – на радио- и проводные телефоны. Последняя категория оргтехники является основным средством связи в любом современном офисе. Мобильной связью признается любая радиосвязь (сотовая, пейджинговая, транковая, рации и др.), которая позволяет абоненту выполнять коммуникативные функции без привязки к определенному месту. Факсимильные средства связи (факс, ПК с факс-модемом) позволяют передавать изображения по телефонному каналу (радио- или проводному). 2. Электронные. К этому классу относятся такие устройства, как персональный компьютер, ноутбук, нетбук и т. п. Как правило, через них координируется работа некоторых других видов оргтехники (в частности сканера, принтера). 3. Печатающие. Печатные машинки сегодня практически канули в лету и используются в настоящее время, наверное, только любителями (к примеру, писателями, привыкшими работать по старинке). Теперь их удачно и эффективно заменило сочетание компьютера и принтера. Принтер представляет собой периферийное компьютерное устройство, которое

используется для вывода нужной информации на бумажный или другой (пластик, ткань) носитель. В зависимости от используемого способа печати эта аппаратура делится на три класса: струйные, матричные и лазерные принтеры. 4. Множительные. Копировальная оргтехника – это копировальные машины, сканеры, ризографы, которые значительно упрощают процесс размножения документов. В общем, принцип работы таких устройств сводится к считыванию исходной информации с листа (текста, рисунка, фотографии), ввода ее в компьютер (в отличие от сканеров ксероксы работают без этого этапа), распознавания и вывода в заданном количестве копий. Ризограф используется для создания брошюр, буклетов, рекламных материалов большим тиражом, размножение которых представляется трудоемким для копировальных аппаратов и экономически невыгодным для профессиональных типографий.

2.1.3 Результаты и выводы:

Принтеры предназначены для вывода информации на твердые носители, большей частью на бумагу. Существует большое количество разнообразных моделей принтеров, которые различаются по принципу действия, интерфейсу, производительности и функциональным возможностями. По принципу действия различают: матричные, струйные и лазерные принтеры.

Сканер - это устройство, позволяющее вводить в компьютер черно-белое или цветное изображения, считывать графическую и текстовую информацию. Сканер используют в случае, когда возникает потребность ввести в компьютер из имеющегося оригинала текст и/или графическое изображение для его дальнейшей обработки (редактирование и т.д.). Ввод такой информации с помощью стандартных устройств ввода требует много времени. Сканированная информация после обрабатывается с помощью специального программного обеспечения (например, программой FineReader) и сохраняется в виде текстового или графического файла.

Копировальный аппарат относится к устройствам, предназначенным для получения копий с оригиналов, выполненных на различных материалах (бумага, пленка). Работа копировального аппарата основана на принципе ксерографии, который подробно рассмотрен в "Принцип электростатической фотографии".

Современные копировальные аппараты классифицируются по ряду признаков, таким как скорость копирования, формат оригинала и число копии рекомендуемого объёма копирования в месяц. С учетом этого все копировальные аппараты относят к одной из пяти групп:

портативные копировальные аппараты (portable copiers); низкоскоростные машины (low-volume copiers); офисные копиры среднего класса (middle-volume copiers); копиры для рабочих групп (high-volume copiers); специальные копировальные аппараты (полноцветные и инженерные машины).

2.2 Практическое занятие № 4, 5, 6 (6 часов).

Тема: «Понятие электронного документооборота**»**

2.2.1 Задание для работы:

1) Общие принципы передачи информации

2) Кодирование сигналов, виды модуляций, пропускная способность канала

3) Каналы передачи информации

2.2.2 Краткое описание проводимого занятия:

Электронный обмен данными - это реальность, с которой сегодня сталкивается практически каждый. Информационные системы,

компьютерные сети, электронная почта - вот далеко не полный перечень тех средств, с помощью которых происходит обмен данными в электронном виде.

В последнее десятилетие появились и получили распространение новые инструментальные средства эффективного обеспечения управленческих процессов. В том числе речь идет о программном обеспечении, предназначенном для обработки управленческих документов. Здесь прежде всего следует упомянуть программное обеспечение классов "системы управления документами" и "системы управления деловыми процессами" *(112) .

Такие системы представляют собой программные комплексы, применимые для решения ряда задач, в том числе и для построения корпоративных систем электронного документооборота. В рамках автоматизации процесса обработки документа в организации с момента его создания или получения до момента отправки корреспонденту или завершения исполнения и списания в дело должно быть обеспечено решение следующих функций:

- регистрация входящих в организацию документов, исходящих из организации документов и внутренних документов;
- учет резолюций, выданных по документам руководством организации, и постановка документов на контроль;
- централизованный контроль исполнения документов;
- списание документов в дело;
- ведение информационно-справочной работы;
- формирование делопроизводственных отчетов по организации в целом.

Использование системы электронного документооборота позволяет организовать передачу данных о ходе исполнения документов в электронном виде, что качественно меняет организацию контроля исполнения документов.

Карточки зарегистрированных централизованно документов с резолюциями руководства рассылаются в электронном виде сотрудникам соответствующих подразделений. Они дополняют их резолюциями по исполнению документов, выдаваемыми руководителями структурных подразделений. По мере появления данных о ходе исполнения документов эти данные вносятся в систему. При этом система автоматически отслеживает наступление даты предварительного уведомления о приближении срока исполнения и наступление самого этого срока. Заинтересованные пользователи системы информируются о названных сроках.

Также значительно видоизменяется процесс согласования проектов документов, в рамках которого сотрудники, участвующие в процессе согласования, получают возможность обмениваться электронными версиями согласуемых проектов. Такая технология позволяет сократить время, затрачиваемое на передачу проектов в бумажном виде.

Система электронного документооборота обязательно включает текущий электронный архив, который решает проблемы оперативного доступа к информации и наличия возможности одновременного использования документа несколькими сотрудниками. Такая форма организации хранения значительно снижает вероятность потери информации и повышает оперативность работы за счет сокращения времени поиска нужного документа. Хранение текстов документов в электронном виде позволяет реализовывать полнотекстовый поиск, что открывает принципиально новые возможности при ведении информационно-справочной работы, например, позволяет делать тематические подборки документов по их содержанию. Использование электронного архива избавляет от необходимости создавать фонд пользования архивных документов, так как по запросу в любой момент может быть выдана электронная копия документа.

2.2.3 Результаты и выводы:

Обмен информацией производится по каналам передачи информации. Каналы передачи информации могут использовать различные физические принципы. Так, при непосредственном общении людей информация передается с помощью звуковых волн, а при разговоре по телефону - с помощью электрических сигналов, которые распространяются по линиям связи. Компьютеры могут обмениваться информацией с использованием каналов связи различной физической природы: кабельных, оптоволоконных, радиоканалов и др.

Передача сообщений по радиоканалу осуществляется путем изменения параметров несущего колебания под воздействием информационного сообщения. При передаче аналоговых сигналов эти параметры изменяются непрерывно и пропорционально их уровню; при передаче цифровых сигналов в зависимости от значений одного или нескольких информационных символов осуществляется манипуляция параметров несущего колебания, то есть они принимают определенные фиксированные значения.

Для построения компьютерных сетей применяются линии связи, использующие различную физическую среду. В качестве физической среды в коммуникациях используются: металлы (в основном медь), сверхпрозрачное стекло (кварц) или пластик и эфир. Физическая среда передачи данных может представлять собой кабель "витая пара", коаксиальные кабель, волоконно-оптический кабель и окружающее пространство.

Линии связи или линии передачи данных - это промежуточная аппаратура и физическая среда, по которой передаются информационные сигналы (данные).

В одной линии связи можно образовать несколько каналов связи (виртуальных или логических каналов), например путем частотного или временного разделения каналов. Канал связи - это средство односторонней

передачи данных. Если линия связи монопольно используется каналом связи, то в этом случае линию связи называют каналом связи.

2.3 Практическое занятие № 7, 8, 9 (6 часов).

Тема: «Устройства создания электронных документов**»**

2.3.1 Задание для работы:

1) Компьютер: текстовые и табличные процессоры

2) Объектно-ориентированные среды формирования документов

3) Телеграф, телекс, телетекст

2.3.2 Краткое описание проводимого занятия:

Создание простых текстовых документов может выполняться на пишущих машинках различного вида с последующим вводом текста с бумажного документа в ПК с помощью сканера. Но, безусловно, эффективнее даже простые документы создавать непосредственно на ПК с использованием широкого арсенала программных средств, обеспечивающих удобный и высокоэффективный сервис. Тем боле

е этот сервис важен при создании сложных высокохудожественных документов, предназначенных для последующего тиражирования. Составление таких сложных документов требует исполнения процедур набора текста, редактирования, корректуры, подготовки иллюстраций, макетирования и верстки страниц, печати.

Часто непосредственными источниками материалов для документов служат системы) сканирования изображений, факсы, электронная почта, электронные таблицы, графики, чертежи и т.п.

Все процедуры создания документа можно эффективно выполнить на ПК, оснащенной сканером и набором проблемно-ориентированных ППП, в

первую очередь программ текстового редактирования или настольной издательской системы. Сканер может использоваться для ввода в документ отдельно подготовленных фрагментов: рисунков, фотографий, схем, печатей, подписей и др.

Пример 7.23. В системах управления электронными документами можно использовать; текстовые редакторы: Лексикон, Muiti Edit, Word Perfect, Word 7.0; художественные редакторы: Page Maker, Water Mark Professional; издательские системы; Ventura Publisher, Corel Draw, Frame Maker; редакторы изображений, получаемых от сканеров: Water Mark Professional, Photo Styler, Photo Shop, и многие другие программные продукты.

Хранение электронных документов. Система хранения электронных документов должна обеспечить эффективное хранение и актуализацию документов во внешней памяти ЭВМ, а также их эффективный поиск и конфиденциальный доступ к ним. Хранилищем специальным образом организованной информации, в том числе и электронных документов, во внешней памяти ЭВМ являются базы данных. Для создания и обслуживания баз данных предназначены системы управления базами данных, которые подробно рассмотрены в гл.15.

Манипулирование электронными документами. Основными функциями этой подсистемы являются: организация работы с электронными документами, контроль исполнения документов, их электронное распространение, распечатка и тиражирование.

2.3.3 Результаты и выводы:

Табли́чный проце́ссор —категория программного обеспечения, предназначенного для работы сэлектронными таблицами. Изначально табличные редакторы позволяли обр абатывать исключительнодвухмерные таблицы, прежде всего с числовыми да

нными, но затем появились продукты, обладавшиепомимо этого возможност ью включать текстовые, графические и другие мультимедийные элементы.Ин струментарий электронных таблиц включает мощные математические функц ии, позволяющие вестисложные статистические, финансовые и прочие расче ты.

Электро́нные табли́цы (или табличные процессоры) - это прикладные программы, предназначенные дляпроведения табличных рас четов. Появление электронных таблиц исторически совпадает с началомрасп ространения персональных компьютеров. Первая программа для работы с эле ктронными таблицами— табличный процессор, была создана в 1979 году, предназначалась для компь ютеров типа Apple II иназывалась VisiCalc. В 1982 году появляется знаменит ый табличный процессор Lotus 1-2-3,предназначенный для IBM PC. Lotus объединял в себе вычислительные воз можности электронных таблиц,деловую графику и функции реляционной СУ БД. Популярность табличных процессоров росла оченьбыстро. Появлялись н овые программные продукты этого класса: Multiplan, Quattro Pro, SuperCalc и другие.Одним из самых популярных табличных процессоров сегодня являет ся MS Excel, входящий в составпакета Microsoft Office.

Телеграф - способ передачи кодированной побуквенно информации по проводам. Первоначально специальным кодом (Морзе, Бодо и другими), затем кодом, унифицированным с ЭВМ и другими средствами хранения информации (МТК-2, КОИ-7 и др.), что позволило посылать при помощи не ключа, а клавиатуры, а принимать не в виде точек и тире на ленте, а в виде напечатанных букв. Ранее употреблялся также неэлектрический (оптический) телеграф.

Телетайп это лишь одна из марок (копирайт фирмы Teletype) буквопечатающего аппарата, ставшая общим названием (как ксерокс - из фирменной марки Xerox в общее понятие), и более распространены другие модели телеграфных аппаратов (СТК-2, сохранившийся в почтовых

отделениях и особенный печатанием не на лист, а на наклеиваемую затем ленту, а также использованием 5-, а не 7-битного кода, Т-63, Т-100 и др.).

Телефакс - понятие иного логического ряда. Это система передачи изображений, а не буквенных сообщений, используя обычную (телефонную) сеть. Факс класса 1 (фототелеграф) использовал телеграфные линии и, как правило, приём на фотобумагу, в настоящее время практически вымер. Факс класса 3 и 4 (класс 2 не нашёл употребления) использует передачу в полосе телефонной связи с использованием квадратурного кодирования и специализированный алгоритм сжатия изображений.

2.4 Практическое занятие № 10, 11, 12 (6 часов).

Тема: «Физические среды и протоколы передачи данных**»**

2.4.1 Задание для работы:

1) Модем и его протоколы

2) FAX-протоколы

3) Протоколы локальных сетей физического уровня: Ethernet, ARCnet, Token Ring.

2.4.2 Краткое описание проводимого занятия:

Физическая среда является основой, на которой строятся физические средства соединения. Сопряжение с физическими средствами соединения посредством физической среды обеспечивает Физический уровень. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц. На физическом уровне находится носитель, по которому передаются данные. Среда передачи данных может включать как кабельные, так и беспроводные технологии. Хотя физические кабели являются наиболее распространенными носителями для сетевых коммуникаций, беспроводные

технологии все более внедряются благодаря их способности связывать глобальные сети.

На физическом уровне для физических кабелей определяются механические и электрические (оптические) свойства среды передачи, которые включают:

- тип кабелей и разъемов;

- разводку контактов в разъемах;

- схему кодирования сигналов для значений 0 и 1.

Канальный уровень определяет доступ к среде и управление передачей посредством процедуры передачи данных по каналу. В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

Кабели связи, линии связи, каналы связи

Для организации связи в сетях используются следующие понятия:

- кабели связи;

- линии связи;

- каналы связи.

Из кабелей связи и других элементов (монтаж, крепеж, кожухи и т.д.) строят линии связи. Прокладка линии внутри здания задача достаточно серьезная. Длина линий связи колеблется от десятков метров до десятков тысяч километров. В любую более-менее серьезную линию связи кроме кабелей

входят: траншеи, колодцы, муфты, переходы через реки, море и океаны, а также грозозащита (равно как и другие виды защиты) линий. Очень сложны охрана, эксплуатация, ремонт линий связи; содержание кабелей связи под избыточным давлением, профилактика (в снег, дождь, на ветру, в траншее и в колодце, в реке и на дне моря). Большую сложность представляют собой юридические вопросы, включающие согласование прокладки линий связи, особенно в городе. Вот чем линия (связи) отличается от кабеля.

По уже построенным линиям организуют каналы связи. Причем если линию, как правило, строят и сдают сразу всю, то каналы связи вводят постепенно. Уже по линии можно дать связь, но такое использование крайне дорогостоящих сооружений очень неэффективно. Поэтому применяют аппаратуру каналообразования (или, как раньше говорили, уплотнение линии). По каждой электрической цепи, состоящей из двух проводов, обеспечивают связь не одной паре абонентов (или компьютеров), а сотням или тысячам: по одной коаксиальной паре в междугородном кабеле может быть образовано до 10800 каналов тональной частоты (0,3–3,4 КГц) или почти столько же цифровых, с пропускной способностью 64 Кбит/с.

При наличии кабелей связи создаются линии связи, а уже по линиям связи создаются каналы связи. Линии связи и каналы связи заводятся на узлы связи. Линии, каналы и узлы образуют первичные сети связи.

2.4.3 Результаты и выводы:

Модем– это устройство для обмена информации с другими компьютерами через сеть (телефонную).

Факс-модем– это устройство сочетающее возможности модема и средства для обмена факсимильными сообщениями с другими факс – модемам и обычными телефонными аппаратами.

Модемы – это устройства предназначенные для передачи информации через телефонную сеть.

Модем – это устройство прямого(модулятор) и обратного(демодулятор) преобразования сигнала принятого для использования в определенном канале связи.

Модем преобразует цифровой сигнал в аналоговый, этот процесс называется модуляцией, обратный процесс – демодуляцией.

IBM-модем-телефонная сеть-модем-IBM

Цифровые данные поступающие в модем из компьютера преобразуются в нем путем модуляции и направляются в телефонную линию. Модем-приемник принимает данные по протоколу осуществляет обратное преобразование и пересылает восстановленные цифровые данные в свой компьютер.

Протоколы MNP -протоколы коррекции ошибок нижнего уровня.

При передаче данных по зашумленным телефонным линиям, как уже говорилось выше, всегда существует вероятность, что данные, передаваемые одним модемом, будут приняты другим модемом в искаженном виде - некоторые передаваемые байты могут изменить свое значение или даже просто исчезнуть.

Для того, чтобы пользователь имел гарантии, что его данные переданы без ошибок, используются протоколы коррекции ошибок.

Общая форма передачи данных по протоколам с коррекцией ошибок следующая: данные передаются отдельными блоками (пакетами) по 16-20000 байт, в зависимости от качества связи. Каждый блок снабжается заголовком, в котором указана проверочная информация, например контрольная сумма

блока. Принимающий компьютер самостоятельно подсчитывает контрольную сумму каждого блока и сравнивает ее с контрольной суммой из заголовка блока. Если эти две контрольный суммы совпали, принимающая программа считает, что блок передан без ошибок. В противном случае принимающий компьютер передает передающему запрос на повторную передачу этого блока.

Протоколы коррекции ошибок могут быть реализованы как на аппаратном уровне, так и на программном. Аппаратный уровень реализации более эффективен. Быстродействие аппаратной реализации протокола MNP примерно на 30% выше, чем программной.

2.5 Практическое занятие № 13, 14, 15, 16 (8 часов).

Тема: «Безопасность в вычислительных сетях.**»**

2.5.1 Задание для работы:

1) Аппаратные и программные средства защиты информации

2) Криптография

3) Шифрование с секретными ключами

4) Шифрование с открытыми ключами

2.5.2 Краткое описание проводимого занятия:

Цели защиты информации в сетях сводятся к обеспечению целостности (физической и логической) информации, а также предупреждение несанкционированной ее модификации, получения и размножения. Задачи защиты информации в компьютерных сетях определяются теми угрозами, которые потенциально возможны в процессе их функционирования, в частности:

- *прослушивание каналов*, т.е. запись и последующий анализ всего проходящего потока сообщений;
- *умышленное уничтожение или искажение* (фальсификация) информации;
- *присвоение злоумышленником чужого идентификатора* своему узлу или ретранслятору;
- *преднамеренный разрыв линии связи*, что приводит к полному прекращению доставки сообщений;
- *внедрение сетевых вирусов*.

Т.о. специфические задачи защиты информации в сети состоят в следующем:

- *конфиденциальность (маскировка данных)* – предотвращение пассивных атак для передаваемых или хранимых данных;
- *арбитражное обеспечение,* т.е. защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных.
- *аутентификация объектов,* заключающая в подтверждении подлинности взаимодействующих объектов;
- *контроль доступа,* т.е. защита от несанкционированного использования ресурсов сети;
- *контроль и восстановление целостности* находящихся в сети данных;
- *доступность* - защита от потери или снижения доступности того или иного сервиса.

Для решения этих задач создаются специальные механизмы защиты, т.н. сервисы безопасности, которые в общем случае могут быть представлены следующим образом: *идентификация/аутентфикация; разграничение доступа; протоколирование/аудит; экранирование; тунелирование;*

шифрование; контроль целостности; контроль защищенности; обнаружение отказов и оперативное восстановление и управление.

Применительно к различным уровням семиуровнего протокола передачи данных задачи конкретизируются следующим образом:

- На *физическом уровне* – контроль электромагнитных излучений линий связи и устройств, поддержка коммутационного оборудования в рабочем состоянии (экранирующие устройства, генераторы помех, средства физической защиты передающей среды).
- На *канальном уровне* – это шифрование данных.
- *Сетевой уровень* – наиболее уязвимый, поскольку сетевые нарушения (чтение, модификация, уничтожение, дублирование, переориентация, маскировка под другой узел) осуществляются и использованием его же протоколов. Здесь основой защиты выступают средства криптографии.
- На *транспортном уровне* все активные угрозы становятся видимыми, но, к сожалению, не все угрозы можно предотвратить криптографическими методами, анализом регулярности трафика и посылкой параллельных дубликатов сообщений по другим путям, используемыми на данной уровне.
- Протоколы *сеансового* и *представительного* уровня функций защиты практически не выполняют.
- В функции защиты протокола *прикладного уровня* входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей и другие функции, определенные конкретным протоколом. Более сложными эти функции являются при реализации полномочной политики безопасности в сети.

Практически все механизмы сетевой безопасности могут быть реализованы на третьем уровне эталонной модели ***ISO/OSI***. Более того, ***IP***-уровень считается самым оптимальным для размещения защитных средств,

поскольку при этом достигается компромисс между защищенностью, эффективностью функционирования и прозрачностью для приложений.

Наиболее проработанными являются вопросы защиты на ***IP***-уровне. Спецификации (протоколы) семейства ***IPsec*** (рабочая группа ***IP Security***) обеспечивают: *управление доступом; контроль целостности на уровне пакетов (вне соединения); аутентификацию источника данных; защиту от воспроизведения; конфиденциальность (включая частичную защиту от анализа трафика); администрирование (управление криптографическими ключами).*

2.5.3 Результаты и выводы:

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая ***криптографией*** [от греч. ***kryptos***- скрытый и ***grapho*** - пишу].

Системы шифрования могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков. К программам первого типа можно отнести архиваторы типа ARJ и RAR, которые позволяют использовать криптографические методы для защиты архивных файлов. Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities, Best Crypt.

Аппаратно-программные средства защиты информации можно разбить на пять групп:

6. Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.
7. Системы шифрования дисковых данных.
8. Системы шифрования данных, передаваемых по сетям.

9. Системы аутентификации электронных данных.
10. Средства управления криптографическими ключами.

Различают два основных способа шифрования: канальное шифрование и оконечное (абонентское) шифрование.

В случае ***канального шифрования*** защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством - встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы. Однако у данного подхода имеются и существенные недостатки:

- шифрование служебных данных осложняет механизм маршрутизации сетевых пакетов и требует расшифрования данных в устройствах промежуточной коммуникации (шлюзах, ретрансляторах и т.п.);
- шифрование служебной информации может привести к появлению статистических закономерностей в шифрованных данных, что влияет на надежность защиты и накладывает ограничения на использование криптографических алгоритмов.

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации данных применяют код аутентификации сообщения (имитовставку) или электронную подпись.

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети.

Различают следующие виды функций управления ключами: генерация, хранение, и распределение ключей.